(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 380 831**

(51) Int. CI.:
H04N 1/44 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Número de solicitud europea: **07846730 .5**
(96) Fecha de presentación: **22.11.2007**
(97) Número de publicación de la solicitud: **2210406**
(97) Fecha de publicación de la solicitud: **28.07.2010**

(54) Título: **Método y aparato que permite una transmisión asegurada de facsimil**

(45) Fecha de publicación de la mención BOPI:
18.05.2012

(45) Fecha de la publicación del folleto de la patente:
18.05.2012

(73) Titular/es:
PURELLA AG
C/O REVIDES TREUHAND AG
INDUSTRIESTRASSE 21
6055 ALPNACH DORF, CH

(72) Inventor/es:
STEEGER, Gerd

(74) Agente/Representante:
Lehmann Novo, Isabel

DESCRIPCIÓN

Método y aparato que permite una transmisión asegurada de facsimil

CAMPO TÉCNICO

La invención se refiere a un método para la transmisión asegurada de facsimil según el preámbulo de la reivindicación 1 y a un aparato para la transmisión asegurada de facsimil según el preámbulo de la reivindicación 7. En general, la presente invención pertenece al campo de las tecnologías de telecomunicaciones.

ANTECEDENTES DE LA INVENCIÓN

La transmisión de facsimil suele sustituir al correo ordinario o servicios de entrega tales como UPS® y FedEx®, porque es rápida y fiable y el destinatario puede recibir un mensaje en tan solo unos minutos, en lugar de horas o incluso días o semanas. Con frecuencia, una información reservada, tal como, por ejemplo, planos técnicos a nivel interno, datos financieros o de negocios confidenciales o información privada necesitan transmitirse mediante un dispositivo de transmisión de facsimil. Sin embargo, con frecuencia, un grupo bastante numeroso de personas tiene acceso a una máquina de facsimil, p.e., en una gran oficina o en un hotel. Por lo tanto, predomina la posibilidad de que una persona vea el contenido de una transmisión de facsimil entrante antes del destinatario previsto real, lo que puede dar lugar a una violación del secreto.

Las transmisiones de facsimil se suelen realizar a través de una red pública según una norma de telecomunicaciones definida por el Sector de Normalización de las Telecomunicaciones (ITU-T) de la ITU (Unión Internacional de Telecomunicaciones), anteriormente CCITT (Comité Consultivo Internacional Telefónico y Telegráfico). Las transmisiones según esta normalización son, similares al texto sin cifrar, fáciles de leer y por lo tanto, fáciles de interceptar, lo que representa una ayuda para las actividades del espionaje industrial.

Además, si un facsimil no llega al destinatario previsto debido a, por ejemplo, un error de mecanografiado de su número de facsimil, pulsación de la tecla de marcación rápida errónea o un error en la red telefónica, pero, en cambio, llega a otro destinatario, con lo que los datos transmitidos pueden llegar al poder de destinatarios no deseables.

Por lo tanto, hubo una necesidad de transmisión asegurada de facsimil, en particular para transmisión asegurada de facsimil a través de la red telefónica pública.

El documento US-A-6 014 444 da a conocer un aparato para la comunicación encriptada. El aparato puede ser una máquina de facsimil que comprende una unidad escaneadora para la lectura de un documento que ha de transmitirse, una unidad de impresora, una unidad de procesamiento de datos, una unidad de transmisión de datos con un módem y una unidad de control. El aparato puede ser también un ordenador personal. Los datos de transmisión se transmiten y los datos de recepción se reciben por la unidad de transmisión de datos, a través de un circuito telefónico. Un sensor de imagen de línea CCD de la unidad escaneadora explora el documento para la lectura de los datos en una unidad de líneas. La unidad de procesamiento de datos está constituida por una memoria que almacena los datos de transmisión y de recepción, un circuito de compresión/expansión para comprimir y expandir los datos, un circuito de encriptación/desencriptación para encriptar los datos de transmisión y para desencriptar los datos de recepción y un circuito de procesamiento de datos. La memoria permite la recepción confidencial. El circuito de compresión/expansión puede comprimir los datos de transmisión y expandir los datos de recepción basándose en el sistema de codificación MMR (Lectura Modificada - Modificada) y además, en el sistema de codificación de MH (Huffman Modificada) o MR (Lectura Modificada). El circuito de encriptación/desencriptación encripta y desencripta los datos utilizando una clave de encriptación predeterminada. La unidad de control almacena la clave de encriptación en su memoria RAM y está provista de medios de comprobación de claves de cifrado. La máquina de facsimil del lado de recepción recibe, a través del módem, el texto cifrado enviado desde la máquina de facsimil del lado de transmisión y el texto cifrado recibido se desencripta mediante el circuito de encriptación/desencriptación utilizando la clave de cifrado y se reestablece a los datos iniciales. Los datos reestablecidos al estado inicial son decodificados (expandidos) por el circuito de compresión/expansión y los datos decodificados se envían a la impresora y se imprimen. La unidad de control comprueba si un signo RTC (retorno a control), es decir, un signo unido al final de los datos codificados comprimidos, está contenido en las 50 líneas transmitidas de datos decodificados o no lo está.

El documento US-A-5 692 048 da a conocer un método y un aparato para enviar transmisiones aseguradas de facsimil y transmisiones de facsimil certificadas que proporcionen el escaneado de un documento en una primera serie de valores de datos digitales en una primera localización. La primera serie de valores de datos es objeto de encriptación. Los conjuntos encriptados de valores de datos se envían, a través de una red de comunicaciones, a un segundo emplazamiento. Los valores de datos encriptados se reciben e imprimen en el segundo emplazamiento para generar un documento encriptado. Los valores de datos encriptados se pueden recuperar mediante la función de escaneado y a continuación, su desencriptación. Los datos pueden someterse, además, a funciones de compresión y descompresión.

En el documento US-B1-6 950 213 se describe un aparato de decodificación/re-codificación de fax, que comprende un decodificador sensible a una imagen de fax codificada definida por hileras de líneas de exploración, un dispositivo de

manipulación de líneas de exploración y un re-codificador (re-compresor) para generar una imagen re-codificada. Una presentación de longitud de serie de líneas de exploración se utiliza en lugar de una representación en mapas de bits. Cada línea de exploración se puede representar como una secuencia de longitudes de serie, esto es, una estructura matricial ordenada o una lista de números enteros que representen longitudes de secuencias alternadas de pixels blancos o negros, comenzando con una longitud de serie de pixels blancos. Una codificación en dos dimensiones emplea dos líneas de exploración en cualquier momento dado, una línea de referencia y una línea de codificación, que suelen ser la codificación de longitud de serie de las respectivas líneas de exploración en mapas de bits originales.

El documento EP-A-0 821 516 da a conocer un método de comunicación de facsimil y un dispositivo para generar una imagen de un documento, dividiendo los puntos de la imagen en unidades de un tamaño predeterminado y encriptando la imagen cambiando la posición de las unidades.

DESCRIPCIÓN DETALLADA DE LA INVENCIÓN

Un objetivo de la presente invención es dar a conocer un método y un aparato para la transmisión asegurada de facsimil que sea compatible con los protocolos y normas de facsimil convencionales existentes. Otro objetivo de la invención es dar a conocer un método y un aparato para la transmisión asegurada de facsimil, que pueda emplear máquinas de facsimil convencionales, para enviar y recibir un facsimil. Otro objetivo de la invención es dar a conocer un método y un aparato para la transmisión asegurada de facsimil que estén configurados de modo que solamente el destinatario previsto pueda ver el facsimil recibido, esto es, otras personas distintas al destinatario previsto no pueden ver el facsimil recibido. Otro objetivo de la presente invención es dar a conocer un método y un aparato que estén configurados de modo que el riesgo de interceptar una transmisión en una red pública sea reducido al mínimo o incluso eliminado, mientras que se mantiene la compatibilidad con la red pública y se proporciona facilidad de uso.

Con el fin de poner en práctica estos y otros objetivos de la invención, que se harán más evidentes a medida que prosiga la descripción, se da a conocer un método para la transmisión asegurada de facsimil de un documento, que comprende las etapas de generar al menos una imagen del documento a transmitirse (etapa a)), la lectura de los pixels de la al menos una imagen en una serie de bloques de tamaño predeterminado (etapa b)), la conversión de la serie de bloques en una cadena de caracteres basada en una tabla de conversión (etapa c)), la encriptación de la cadena de caracteres para crear datos cifrados en forma de una cadena de caracteres encriptada (etapa d)), la compresión de la cadena de caracteres encriptada para crear una imagen aleatorizada (lo que significa una imagen comprimida) en forma de datos más pequeños (etapa e)) y la transmisión de la imagen aleatorizada (etapa f)). Para la creación de la imagen aleatorizada, en particular de una imagen codificada de Huffman, la cadena de caracteres generada se convierte de nuevo en una imagen, es decir, de nuevo en pixels. Una opción entre un modo de encriptación estándar y un modo de encriptación optimizado se proporciona en esta forma de realización, en donde en el modo de encriptación estándar, en la etapa a), se genera una imagen a partir del documento completo y en el modo de encriptación optimizado, en la etapa a), se genera una serie de imágenes, correspondiendo cada imagen a una sola línea del documento que se va a transmitir; en la etapa b), los pixels de cada imagen de la serie de imágenes son objeto de lectura en una serie de bloques de tamaño predeterminado, en la etapa c), la serie de bloques correspondientes a cada imagen se convierten, cada una, en una cadena de caracteres, lo que da lugar a una sola cadena de caracteres por imagen y línea y en la etapa d) solamente son objeto de encriptación las cadenas de caracteres correspondientes a las imágenes y líneas con al menos un píxel no blanco. Una línea de un documento puede denominarse también una hilera de un documento.

Además, se da a conocer un aparato para proporcionar una transmisión asegurada de facsímil de un documento, que comprende un dispositivo de transmisión para transmitir un facsimil de un documento. El dispositivo de transmisión comprende medios de generación de imágenes para generar al menos una imagen del documento, una unidad de encriptación para generar una cadena de caracteres encriptada y medios de compresión para comprimir la cadena de caracteres generada para crear una imagen aleatorizada a transmitirse. Para la creación de la imagen aleatorizada, la cadena de caracteres generada se convierte de nuevo en una imagen, esto es, de nuevo en pixels. La unidad de encriptación tiene una memoria para almacenar la al menos una imagen, medios de conversión para la lectura de los pixels de la al menos una imagen en una serie de bloques de tamaño predeterminado y para convertir la serie de bloques en la cadena de caracteres basándose en una tabla de conversión y medios de encriptación para la encriptación de la cadena de caracteres para crear una cadena de caracteres encriptada. Los medios de encriptación están diseñados de modo que se proporcione un modo de encriptación estándar y un modo de encriptación optimizado. En el modo de encriptación estándar, se genera una sola imagen a partir del documento completo por los medios de generación de imágenes. En el modo de encriptación optimizado una serie de imágenes se genera por los medios de generación de imágenes correspondiendo cada imagen a una sola línea del documento. Los pixels de cada imagen de la serie de imágenes son objeto de lectura en una serie de bloques de tamaño predeterminado y la serie de bloques correspondiente a cada imagen y cada línea se convierten, cada una, en una cadena de caracteres por los medios de conversión, dando lugar a una sola cadena de caracteres por imagen y línea. Solamente las cadenas de caracteres correspondientes a imágenes y líneas, con al menos un píxel no blanco, se encriptan luego mediante los medios de encriptación.

Por lo tanto, en el modo de encriptación optimizado, una cadena de caracteres de una imagen de una línea en blanco del documento, esto es, de una línea con solamente pixels blancos, no es encriptada antes de la compresión. Solamente las cadenas de caracteres correspondientes a líneas con al menos un píxel negro son encriptadas antes de la compresión

en el modo de compresión optimizado. Las cadenas de caracteres, correspondientes a líneas en blanco, se dejan sin encriptar, lo que da lugar a un tamaño de imagen global más pequeño y más corto, una alta tasa de compresión y por lo tanto, un tiempo de transmisión corto. En el modo de encriptación estándar, todos los pixels de una línea son encriptados, haciendo caso omiso de si la línea consiste solamente en pixels blancos o no.

En una forma de realización preferida, cualquier máquina de facsimil ordinaria se puede mejorar con dicha unidad de encriptación para obtener el aparato según la invención. Además, se puede utilizar un ordenador personal con un software adecuado para la transmisión de facsimil.

BREVE DESCRIPCIÓN DE LOS DIBUJOS

Otras características y aplicaciones ventajosas de la invención se pueden encontrar en las reivindicaciones dependientes así como en la siguiente descripción de los dibujos que ilustran la invención. En los dibujos, los signos de referencia similares designan las mismas o partes similares a través de las diversas figuras, en donde:

La Figura 1 representa un diagrama de bloques de una forma de realización del aparato según la invención;

Las Figuras 2a y 2b representan un diagrama de flujo que ilustra el envío/transmisión de un documento según una forma de realización del método de la invención;

La Figura 3 representa un diagrama de flujo que ilustra la recepción de un documento según una forma de realización del método de la invención;

Las Figuras 4a y 4b representan un diagrama de flujo que ilustra las etapas b) a d) de una forma de realización del método según la invención para el modo de encriptación estándar y para el modo de encriptación optimizado;

La Figura 5 representa un ejemplo ilustrativo de un marcador que puede añadirse después de la cabecera de un facsimil según una forma de realización del método de la invención;

La Figura 6 representa un ejemplo ilustrativo de un facsimil generado con el método de la invención en el modo de encriptación optimizado que presenta un marcador 200 que constituye un borde entre una cabecera de facsimil (o bandera) y su contenido en forma de una imagen aleatorizada;

La Figura 7 representa otro ejemplo ilustrativo de un facsimil generado con el método de la invención en el modo de encriptación optimizado que presenta un marcador 200 y la

Figura 8 representa un ejemplo ilustrativo de un facsimil generado con el método según la invención, en el modo de encriptación estándar.

FORMAS DE REALIZACIÓN DE LA INVENCIÓN

La Figura 1 representa una forma de realización preferida 10 de un aparato para la transmisión asegurada de facsímil según la invención, estando la forma de realización preferida en el modo de una máquina de facsimil 1. Por supuesto, se puede utilizar también un ordenador personal (PC) como aparato para la transmisión asegurada de facsímil según la invención.

La máquina de facsimil 10 comprende un dispositivo escaneador 12 para explorar los documentos que han de transmitirse (esto es, para la generación de imágenes a partir de documentos que han de transmitirse). El dispositivo de escaneado 12 representa medios de generación de imágenes y es capaz de la lectura de los pixels de un documento a escanearse línea por línea. Si se utiliza un ordenador personal como el aparato para la transmisión asegurada de facsimil, en tal caso, la lectura de los pixels de un documento se realiza por medio de un programa de software adecuado, preferentemente un controlador de dispositivo de escaneado y/o controlador de impresora para crear, en particular, una imagen del grupo 3 de TIFF (Formato de Fichero de Imágenes Etiquetadas).

La máquina de facsimil 10 comprende, en una forma de realización preferida, también un alimentador de documentos (no ilustrado). Comprende, además, un dispositivo de transmisión para transmitir/enviar un facsimil y preferentemente, un dispositivo de recepción para recibir un facsimil. En la forma de realización ilustrada 10, el dispositivo de transmisión y el dispositivo de recepción están formados, a modo de ejemplo, por un solo dispositivo de transmisión y recepción 11. Sin embargo, pueden ser dispositivos independientes.

El dispositivo de transmisión comprende medios de compresión y el dispositivo de recepción comprende medios de expansión. Si se utiliza un dispositivo de transmisión y de recepción 11, en tal caso, los medios de compresión y los medios de expansión están preferentemente formados por medios de compresión y de expansión 14, esto es, están integrados en una sola unidad. Los medios de compresión y/o los medios de expansión se pueden formar mediante un circuito electrónico y/o un programa informático. Pueden cada uno, o juntos, construirse como un módulo independiente. Los medios de compresión y los medios de expansión están preferentemente construidos de modo que puedan

comprimir y expandir los datos en función de la codificación de MR (Lectura modificada) o de MH (Huffman modificada), lo que posibilita transmitir una imagen aleatorizada generada por los medios de compresión de conformidad con lo establecido en los reglamentos de CCITT. La codificación MR o MH se puede comparar con una conversión analógica a digital convencional por analogía. El nivel de compresión depende, preferentemente, de la complejidad de la imagen escaneada del documento que se va a transmitir.

El dispositivo de transmisión y de recepción comprende, además, un módem 16 que está conectado, por intermedio de una unidad de control de red 18, a una línea telefónica 20. Un módem 16 es un dispositivo que modula una señal portadora analógica para codificar la información digital y también demodula dicha señal portadora analógica para decodificar la información transmitida. Para la conexión con la línea telefónica 20, el módem 16 es, en una forma de realización preferida, un así denominado módem de banda de voz, que convierte la información digital en sonidos (esto es, señales analógicas), que se pueden transmitir a través de la línea telefónica 20 y convierte las señales analógicas recibidas en señales digitales que se pueden gestionar por el dispositivo de transmisión y de recepción 11. Para transmitir datos, se realiza una compresión por los medios de compresión 14 para generar una imagen aleatorizada que luego se envía/transmite por el módem 16 y la unidad de control de red 18 a través de la línea telefónica 20. Cuando se reciben datos desde el módem 16, los medios de expansión 14 del dispositivo de recepción 11 expanden o descomprimen, respectivamente, los datos recibidos. Si se utiliza un ordenador personal como un aparato para la transmisión asegurada de facsimil, se puede utilizar un así denominado módem de facsimil.

El módem 16 y la unidad de control de red 18 están, preferentemente, conectados a una unidad central de control 22, en particular, a una unidad central de proceso (CPU), que es parte del dispositivo de transmisión y de recepción 11. La unidad central de control 22 comprende un procesador, en particular un microprocesador y una memoria, que preferentemente consiste en una memoria de acceso aleatorio (RAM) 24 y una memoria de lectura solamente (ROM) 26.

Además, la máquina de facsimil 10 comprende una impresora 28 para crear al menos una copia impresa del facsimil recibido. La impresora 28 puede ser, por ejemplo, una impresora térmica, de láser, de chorro de tinta o matricial. Además, el dispositivo de transmisión y recepción 11 comprende una fuente de alimentación 30 y un panel de operaciones 32 (también denominado interfaz de usuario). El panel de operaciones 32 comprende un monitor de visualización 34 para mostrar las demandas o mensajes de entrada de usuarios y un teclado 36 para las entradas de usuarios, en particular, para la introducción de caracteres por el usuario. De una forma opcional, se puede conectar un lector de tarjetas 38 con el panel de operaciones 32, p.e., para la lectura en una clave secreta (también denominada clave privada) de un sistema de encriptación de claves públicas. Si se utiliza un ordenador personal como el aparato para transmisión asegurada de facsimil, una interfaz de usuario o un panel de operaciones pueden comprender dispositivos de interfaz tales como un monitor, un teclado, un ratón y/o cualquier otro dispositivo de entrada/salida.

El dispositivo de transmisión del aparato 10 comprende, además, una unidad de encriptación para generar una cadena de caracteres encriptada. El dispositivo de transmisión tiene una unidad de desencriptación para desencriptar una imagen aleatorizada recibida. La unidad de encriptación y la unidad de desencriptación se pueden integrar en una sola unidad de encriptación y de desencriptación 39, que forma parte del dispositivo de facsimil y de recepción 11. La unidad de encriptación y/o la unidad de desencriptación se pueden diseñar como un módulo independiente. La unidad de encriptación comprende una memoria 42 para memorizar al menos una imagen escaneada del documento a transmitirse, medios de conversión (no ilustrados) para la lectura de los pixels de la al menos una imagen del documento, que se va a transmitir, en una serie de bloques de tamaño predeterminado y para convertir la serie de bloques en una cadena de caracteres basándose en una tabla de conversión y medios de encriptación para la encriptación de la cadena de caracteres para crear una cadena de caracteres encriptada. La tabla de conversión se almacena preferentemente en la memoria 42 o en los propios medios de conversión. La unidad de desencriptación comprende una memoria 42 y medios de desencriptación para la desencriptación de la cadena de caracteres y medios de conversión para convertir la cadena de caracteres desencriptada en una imagen del documento transmitido. Si la unidad de encriptación y la unidad de desencriptación están integradas en la misma unidad de encriptación y desencriptación 39, en tal caso, comparten, preferentemente, la misma memoria 42 y sus medios de conversión están integrados en un medio de conversión y los medios de encriptación y los medios de desencriptación están integrados en un solo medio de encriptación y desencriptación 40. La memoria 42 es, en una forma de realización preferida, una memoria de acceso aleatorio (RAM) y asiste, preferentemente de forma exclusiva, a los medios de encriptación/desencriptación y/o los medios de conversión.

La unidad de encriptación y desencriptación 39, con su memoria 42, habilita el procedimiento de encriptación de imágenes y la transmisión de facsimil garantizada. Si el aparato 10 se diseña como una máquina de facsimil, los medios de encriptación y/o los medios de desencriptación y/o los medios de conversión respectivos se pueden construir como circuitos electrónicos. Si el aparato 10 está diseñado como un ordenador personal, los medios de encriptación y/o los medios de desencriptación y/o los medios de conversión respectivos se pueden realizar por uno o más programas informáticos.

La unidad central de control 22 controla y/o recibe entradas desde al menos el dispositivo de escaneado 12, la impresora 28, el panel de operaciones 32, los medios de compresión, los medios de expansión, la unidad de encriptación, la unidad de desencriptación (o directamente desde los medios de encriptación y los medios de desencriptación y/o los medios de conversión respectivos no ilustrados) y el módem 16 a través de las líneas 44. Además, controla y tiene acceso a la memoria RAM 24 y a la memoria ROM 26.

Las Figuras 2 a 4 representan diagramas de flujo que ilustran una forma de realización preferida del método para la transmisión asegurada de facsímil según la invención. Las Figuras 2a y 2b representan un diagrama de flujo que ilustra el envío/transmisión de un documento.

En la etapa de toma de decisión 50 se comprueba si un documento ha sido insertado, o no, en un alimentador de documentos (también denominado alimentador de páginas) del aparato 10 según la invención. Si no se ha insertado ningún documento, entonces el método espera la inserción de un documento que ha de transmitirse. Si se ha insertado un documento, entonces el método prosigue con la etapa de entrada 52 y espera una entrada de usuario proporcionando demandas adecuadas en el monitor de visualización 34 del panel de operaciones 32. El usuario puede, en la etapa 52, elegir entre el modo de encriptación estándar y el modo de encriptación optimizado, por ejemplo pulsando una tecla de función específica (p.e., F7) en el panel de operaciones 32 si desea que el documento se transmita en un modo de encriptación optimizado o pulsando la tecla “0” para seleccionar el modo de encriptación estándar y “1” para seleccionar el modo de encriptación optimizado.

Además, el usuario es, en la etapa 52, preferentemente solicitado para indicar si desea, o no, una transmisión asegurada; en particular, si la primera página del documento que ha de transmitirse es una página de portada (es decir, se transmitirá de forma no asegurada) o no lo es. Lo anterior se puede realizar también pulsando las teclas apropiadas en el teclado 56 del panel de operaciones 32, p.e., “1” si el usuario desea una transmisión no asegurada (p.e., si la primera página es una página de portada) y “0” si el usuario desea una transmisión asegurada (p.e., si la primera página no es una página de portada). Si el usuario elige la transmisión no asegurada (p.e., si el usuario caracteriza la primera página como una página de portada), entonces no tendrá lugar ninguna encriptación (p.e., la primera página no será encriptada).

Además, el usuario es, en la etapa 52, preferentemente solicitado para introducir una contraseña (clave privada, clave secreta), que ha acordado con el destinatario o una clave pública. La seguridad de la transmisión depende de la magnitud de la contraseña. La contraseña predeterminada puede comunicarse al destinatario mediante una forma separada y asegurada de comunicación. Por supuesto, puede cambiarse en cualquier momento, p.e., por razones de seguridad. Si se utiliza un sistema/algoritmo de claves simétricas, para la encriptación, entonces el intercambio de contraseña con el destinatario sólo es necesario una vez, puesto que en la siguiente vez el mismo usuario y destinatario desearán transmitir, de forma asegurada, un documento, se puede enviar una lista con varias contraseñas al destinatario (o desde el destinatario al usuario) mediante la transmisión asegurada de facsimil. Como alternativa a la selección de una contraseña por el usuario, se puede poner en práctica un sistema/algoritmo de clave pública. En este caso, el destinatario tiene una clave pública que puede conocerse por cualquiera y una clave privada (clave secreta) que es desconocida por los demás. Solamente la clave privada permite al destinatario abrir/acceder al facsimil transmitido. Sin embargo, cuando se utilizan claves públicas, existe la posibilidad de depósito de seguridad de las claves, esto es, el algoritmo/sistema criptográfico utilizado puede mantener una así denominada “pasarela de puerta posterior” mediante la cual se puede eludir una autenticación normal. Como ejemplos se pueden citar el así denominado sistema criptográfico clipper y el sistema Quicken de software de financiación. Si, por el contrario, se utiliza una gestión de claves simétricas como fue aquí recomendado, entonces no es posible el depósito de seguridad de las claves.

Después de que el usuario haya proporcionado las entradas requeridas en la etapa 52, en la etapa 54 el dispositivo de transmisión marcará e intentará iniciar y establecer una conexión con el dispositivo de recepción, al que habrá de transmitirse el documento, a través del módem 16 y la unidad de control de red 18. A continuación, se establece un canal de comunicaciones entre el dispositivo de transmisión y el dispositivo de recepción (en la así denominada fase de negociación).

Después de que se haya establecido un canal de comunicación, en la etapa 56, el documento a transmitirse es objeto de escaneado, línea por línea, por el dispositivo de escaneado 12 hasta que se haya escaneado el documento completo para crear una imagen del documento (preferentemente, una imagen del grupo 3 TIFF) en conformidad con los reglamentos de la CCITT. Esta imagen está todavía sin comprimir y se proporciona mediante datos de imágenes digitales (pixels).

En la etapa de toma de decisión 58, se comprueba si el usuario ha elegido una transmisión no asegurada en la etapa de entrada 52, como, por ejemplo, para una página de portada. Si se ha elegido una transmisión no asegurada, entonces el método se desplazará a la etapa 64 y la imagen creada se transmite al dispositivo de recepción del destinatario sin que tenga lugar ninguna encriptación, pero después de que se haya comprimido por los medios de compresión, creando una imagen aleatorizada /comprimida, en particular una imagen codificada de Huffman.

Sin embargo, si el usuario ha indicado, en la etapa 52, que desea una transmisión asegurada, la imagen del documento se desplaza y almacena en la memoria 42 de la unidad de encriptación, que es preferentemente una memoria de acceso aleatorio (RAM), en la etapa 60. En la etapa 62, la imagen memorizada se procesa por la unidad de encriptación 39, en donde los pixels de la imagen son objeto de lectura en una serie de bloques de tamaño predeterminado, la serie de bloques se convierte en una cadena de caracteres basada en una tabla de conversión y la cadena de caracteres es encriptada para crear una cadena de caracteres encriptada. La etapa 62 se describirá en detalle con respecto a las Figuras 4a y 4b.

En la etapa 64, la cadena de caracteres cifrada se comprime por los medios de compresión después de que se haya convertido a pixels, con lo que se crea una imagen aleatorizada del documento, preferentemente una imagen de TIFF grupo 3. La imagen aleatorizada se transmite luego al dispositivo de recepción por intermedio de la unidad de control de red 18. En la etapa 66, los ajustes de parámetros de configuración establecidos en la entrada 52, en particular con respecto a la transmisión asegurada, son objeto de reposición a sus valores iniciales.

La Figura 3 representa un diagrama de flujo que ilustra la recepción de un documento según una forma de realización del método en conformidad con la invención. De este modo, la Figura 3 ilustra el lado de recepción. En la etapa 70, el dispositivo de recepción espera y reconoce el anillo y la denominada negociación, handshake, del dispositivo de transmisión (esto es, su módem/unidad de control de red). Después de que se haya establecido un canal de comunicación con el dispositivo de transmisión, los datos transmitidos (facsimil), se reciben en forma de una imagen aleatorizada del documento. La imagen aleatorizada se expande luego por los medios de expansión.

En la etapa de toma de decisión 72, se determina si la transmisión ha sido, o no, una transmisión asegurada. Si se determina que no ha tenido lugar ninguna transmisión asegurada, entonces el método prosigue directamente con la etapa 80 e imprime la imagen aleatorizada expandida en la impresora 28. Si se determina que ha tenido lugar una transmisión asegurada, entonces el método prosigue con la etapa 74 y la imagen aleatorizada expandida se almacena en la memoria asignada específica 42 a la que tiene acceso la unidad de desencriptación. La imagen aleatorizada expandida adopta la forma de una cadena de caracteres. Para un procesamiento adicional de esta cadena de caracteres, que está codificada, se solicita al usuario que introduzca una contraseña en la etapa 76. Si la contraseña es correcta, entonces la cadena de caracteres se procesa en la etapa 78 por intermedio de la unidad de desencriptación, esto es, la cadena de caracteres se desencripta por los medios de desencriptación de la unidad de desencriptación y a continuación, la cadena de caracteres desencriptada se convierte en una imagen del documento transmitido por los medios de conversión. Esta imagen se imprime luego, en la etapa 80, como una copia legible. El procesamiento realizado por la unidad de desencriptación corresponde esencialmente a la inversión del procesamiento realizado por la unidad de encriptación que se describe a continuación con referencia a las Figuras 4a y 4b.

Las Figuras 4a y 4b representan un diagrama de flujo que ilustra las etapas b) a d) de una forma de realización del método según la invención para el modo de encriptación estándar y para el modo de encriptación optimizado.

Una vez que se haya desplazado la imagen escaneada, en la etapa 60 (con referencia a la Figura 2b) en la memoria 42, en la etapa 100 la contraseña es objeto de un algoritmo criptográfico para convertirse en una cadena larga de caracteres asegurada 20 (20 caracteres x bits/carácter = 160 bits). Esta cadena de caracteres larga 20 puede, en una forma de realización preferida, comprender todos los 256 caracteres de la tabla ASCII. Un algoritmo criptográfico de hash, tal como, por ejemplo, el SHA-1 (Algoritmo de Hash Seguro 1) puede utilizarse para el proceso criptográfico, hashing, de la contraseña, que se suele proporcionar por una combinación de caracteres que son accesibles en un teclado (esto es, una combinación a partir de 96 caracteres), en una cadena larga de 20 bytes, que se combina a partir de todos los caracteres de la tabla ASCII. Para una clave larga de 160 bits, existen 2^160 posibilidades. Por supuesto, se pueden utilizar otros algoritmos criptográficos.

La siguiente etapa 102 representa el punto de inicio del proceso de encriptación realizado por la unidad de encriptación, en donde cada línea de al menos una imagen, esto es, los pixels de cada línea, es objeto de lectura para bloques de 8 bits, creando una serie de bloques. Cada bloque de 8 bits se convierte luego mediante un desplazamiento de bits en un carácter ASCII, en particular, un carácter ASCII de 8 bits, por los medios de conversión, con lo que se crea una cadena de caracteres ASCII. Un carácter se suele representar por 8 bits o 1 byte, respectivamente. Las líneas de facsimil estándar, en una página de 8,5 pulgadas (21,59 cm) de anchura, se representan cada una por 1728 pixels que se convierten en 216 caracteres o bytes, independientemente de si se utiliza un tamaño US letter o DIN A4 como formato. El número de líneas varía, pero suele ser de 1024 para un tamaño de US letter o según TIFF grupo 3, que se proporciona actualmente por la mayor parte de las máquinas de facsimil. El proceso de encriptación difiere dependiendo de la elección del modo de encriptación.

En la etapa de toma de decisión 104, se determina si el usuario ha elegido, en la etapa 52, el modo de encriptación estándar o el modo de encriptación optimizado. La etapa 105 se refiere al modo de encriptación estándar. En el modo de encriptación estándar, el documento completo a transmitirse es objeto de escaneado de una sola vez, con lo que se realiza un escaneado inmediato de todas las líneas del documento. La totalidad de los pixels de todas las líneas son objeto de lectura, línea por línea, en bloques de 8 bits y se convierten en una sola cadena de caracteres, haciendo caso omiso de si una línea comprende solamente pixels blancos o no. Los 216 caracteres de una línea posterior se añaden a la cadena de caracteres, que contiene los caracteres correspondientes a las líneas precedentes, hasta que todas las líneas sean leídas y convertidas en caracteres, con lo que se crea una sola cadena de caracteres. El número de líneas varía, pero suele ser de 1024. Con 216 caracteres por línea y 1024 líneas, existen 221184 caracteres o bytes, respectivamente, lo que da lugar a una cadena de caracteres con una longitud de 221184 bytes. Si el número de líneas es igual a la variable L, entonces la longitud de la cadena de caracteres es 216 x L. La cadena de caracteres es objeto, luego, de encriptación por un algoritmo de encriptación adecuado, utilizado por los medios de encriptación. El algoritmo de encriptación puede ser cualquier algoritmo de encriptación ya conocido y establecido. El modo de encriptación estándar ofrece un más alto nivel de seguridad que el modo de encriptación optimizado.

Si se elige el modo de encriptación optimizado, en la etapa 106, se genera una serie de imágenes a partir del documento que ha de transmitirse, correspondiendo cada imagen a una sola línea del documento, los pixels de cada imagen son objeto de lectura en bloques de 8 bits y los bloques de 8 bits se convierten en una cadena de caracteres, dando lugar así a una sola cadena de caracteres por imagen y línea. Las operaciones realizadas en la etapa 106 se explican con más detalle en las etapas 120 a 128 representadas en la Figura 4b, siendo la etapa 122 explicada más adelante.

En la etapa 120, se determina si la cadena de caracteres, actualmente procesada, corresponde a una línea en blanco, esto es, si la cadena de caracteres consiste en 216 veces el carácter “0”. Las cadenas de caracteres que corresponden a líneas con pixels exclusivamente blancos no son encriptadas; es decir, solamente las cadenas de caracteres correspondientes a imágenes/líneas con al menos un píxel no blanco son encriptadas en la etapa 124 por los medios de encriptación utilizando preferentemente un algoritmo de encriptación establecido para crear una cadena de caracteres encriptada. Las líneas en blanco no son encriptadas. Las cadenas de caracteres se añaden consecutivamente en la etapa 126. Es decir, las cadenas de caracteres encriptadas, correspondientes a líneas no en blanco y las cadenas de caracteres no encriptadas correspondientes a líneas en blanco, que consisten completamente en el carácter “0”, se añaden en el orden en que aparecen para formar una sola cadena de caracteres. En la etapa 128, se comprueba si la última línea de la imagen ha sido alcanzada y procesada.

La compresión de la cadena de caracteres final (después de que se haya convertido en pixels, esto es, una serie de bits) que tiene lugar en la etapa 64 (con referencia a la Figura 2b), que se realiza, en una forma de realización preferida, en función de la codificación de MH (Huffman modificada) se debe a la naturaleza de la cadena de caracteres final eficiente, lo que da lugar a un pequeño tamaño de facsimil para un tiempo de transmisión corto. La codificación MH resulta eficiente si numerosos bloques de pixels son blancos o negros. Una longitud de serie de 951 pixels blancos corresponde a un código de formación de “0 1101 0011” y un código de terminación de “0101 1000”, que son más cortos que 951 bits. En una forma de realización preferida, la longitud de serie se mantiene en conformidad con los reglamentos de MH (Huffman modificado). Como alternativa, por ejemplo, la codificación MR (lectura modificada) se puede utilizar para la compresión. La compresión realizada por la codificación MH o MR garantiza que se transmita un facsimil en conformidad con los reglamentos de la CCITT.

Cuando la cadena de caracteres, correspondiente a una imagen de una línea con no solamente pixels blancos, es objeto de encriptación, entonces la contraseña se extiende preferentemente mediante una cadena, que se genera basándose en el número de esa línea específica. En la etapa 120 (con referencia a la Figura 4b), se ha determinado si la cadena de caracteres, actualmente procesada, corresponde a una línea en blanco, esto es, si la cadena de caracteres consiste en 216 veces el carácter “0”. Si éste no es el caso, entonces en la etapa 122 (que se realiza en la etapa 120 y 124) se calcula un número pseudo-aleatorio sobre la base del número de fila/línea actual. Este número pseudo-aleatorio es cifrado, preferentemente mediante el mismo algoritmo de cifrado que la contraseña y se añade a la contraseña cifrada. Si la contraseña no se extiende de tal modo, el facsímil puede mostrar un modelo particular que es legible para cualquiera aunque haya tenido lugar una encriptación.

Para la encriptación, se utiliza preferentemente un sistema/algoritmo de gestión de claves simétricas con un cifrado de flujo de tamaños de claves variables. En otra forma de realización preferida, el algoritmo RC4 (código de Ron 4) se utiliza para la encriptación de la cadena de caracteres por los medios de encriptación. Por supuesto, se pueden utilizar otros algoritmos de encriptación/criptográficos adecuados, tales como, por ejemplo, el así llamado Blowfish. El algoritmo RC4 es esencialmente inmune al análisis criptográfico diferencial y lineal. El algoritmo RC4 ofrece 2^1700 (256 x 256^2) estados diferentes y es un algoritmo muy rápido.

Con el fin de poder determinar dónde finaliza una posible cabecera de un facsimil y dónde se inicia el mensaje o documento real, se crea preferentemente un marcador 200 en la etapa 108 (con referencia a la Figura 4a). En la etapa 110, la cadena de caracteres encriptada, que representa el documento, se añade luego al marcador 200 o viceversa, de modo que el marcador 200 esté situado al principio o antes de la cadena de caracteres encriptada, respectivamente. El marcador 200 puede ser cualquier configuración de bits, en particular en forma de una cadena.

La Figura 5 representa un ejemplo de un marcador de 32 bits 200. En la etapa 112, la cadena de caracteres encriptada con el marcador 200, que esencialmente es una cadena de caracteres ASCII, se convierte de nuevo en pixels, que luego se comprimen y transmiten en la etapa 64, preferentemente con la resolución establecida en 200 dpi (puntos por pulgada).

En las Figuras 6 y 7 se representan ejemplos ilustrativos de facsimil recibidos, que han sido generados en el modo de encriptación optimizado. En la Figura 6, el documento ha sido enviado con una cabecera “XYZ” que no ha sido encriptada y se ha añadido un marcador 200. En la Figura 7, el documento fue enviado sin una cabecera a través de la red pública con un marcador 200 en su inicio.

La Figura 8 representa un ejemplo ilustrativo de un facsimil recibido, que ha sido generado en el modo de encriptación estándar, pero que no ha sido expandido ni desencriptado por la unidad de desencriptación, puesto que el destinatario no introdujo la contraseña correcta ni utilizó el hardware correcto. La imagen completa está todavía aleatorizada y no expandida y por ello, es la salida impresa. No puede ser objeto de lectura.

En la presente invención, el dispositivo de transmisión y/o el dispositivo de recepción pueden ser máquinas de facsimil y/o ordenadores personales (PCs) que tienen la capacidad de transmitir y/o recibir un facsimil en conformidad con un estándar de transmisión de facsimil establecido. Lo mismo es verdadero para el aparato según la invención.

El método y el aparato, según la invención, tiene las ventajas de ser fácil de gestionar por un usuario y fácil de poner en práctica por el sector de las máquinas de facsimil. Puesto que las imágenes de los documentos, que preferentemente son imágenes TIFF Grupo 3, están todavía codificadas en conformidad con los reglamentos de la CCITT, el método y el aparato de la presente invención se pueden combinar con máquinas de facsimil ya existentes. Además, las máquinas de facsimil existentes se pueden reconstruir fácilmente para el aparato según la invención (o su dispositivo de transmisión y/o de recepción) añadiendo una unidad de encriptación/desencriptación. La homologación está garantizada puesto que las máquinas de facsimil existentes pueden confirmar que los documentos transmitidos se recibieron en forma adecuada.

Para la desencriptación, no hay necesidad de imprimir el facsimil recibido, ni de escanear la salida impresa y luego proceder a su desencriptación para poder proceder a su lectura. La desencriptación se puede realizar directamente por la unidad de desencriptación. Una cabecera de fax puede permanecer desencriptada, de modo que permanezca legible. El usuario puede elegir preferentemente si desea tener la primera página, que suele ser una página de portada, para llegar a encriptarse o no.

En una forma de realización preferida, el dispositivo de recepción mantiene el facsimil almacenado en una memoria específica hasta que el destinatario previsto introduzca la contraseña correcta, por ejemplo pulsando una tecla de función específica. Por lo tanto, no existe necesidad de acordar un tiempo específico para el envío del facsimil, en el que el destinatario ha de estar presente en el dispositivo de recepción, lo que puede resultar muy inconveniente desde el punto de vista operativo, en particular si el dispositivo de recepción está ocupado por varias personas.

El método, según una realización preferida de la invención, permite al usuario elegir entre dos modos de encriptación diferentes. El primer modo de encriptación es el modo de encriptación estándar, en donde la imagen completa de un documento es encriptada haciendo caso omiso de si existen, o no, líneas en blanco, esto es, líneas con exclusivamente pixels blancos.

El modo de encriptación estándar ofrece un alto, si no el más alto, nivel de seguridad. El segundo modo de encriptación es el modo de encriptación optimizado, en donde el medio/unidad de encriptación toma en consideración si una línea de una imagen escaneada consiste solamente en pixels blancos o no. Las líneas, con pixels exclusivamente blancos, no son encriptadas.

Ha de entenderse que aunque han sido ilustradas y descritas algunas formas de realización de la presente invención, esta última no está limitada a las formas de realización específicas aquí descritas e ilustradas.

REIVINDICACIONES

1. Un método para la transmisión asegurada de facsímil de un documento, que comprende las etapas de:

a) generar al menos una imagen de dicho documento,

b) lectura de los pixels de dicha al menos una imagen en una serie de bloques de tamaño predeterminado,

c) convertir dicha serie de bloques en una cadena de caracteres basada en una tabla de conversión,

d) encriptar dicha cadena de caracteres para crear una cadena de caracteres encriptada,

e) después de que se haya convertido a pixels, comprimir dicha cadena de caracteres encriptada creando, de este modo, una imagen aleatorizada y

f) transmitir dicha imagen aleatorizada,

caracterizado porque el método comprende, además, la etapa de seleccionar entre un modo de encriptación estándar y un modo de encriptación optimizado, en donde en el modo de encriptación estándar, en la etapa a), se genera una imagen a partir del documento completo y en el modo de encriptación optimizado, en la etapa a) se genera una serie de imágenes, correspondiendo cada imagen a una sola línea del documento, en la etapa b) los pixels de cada imagen de dicha serie de imágenes son objeto de lectura en una serie de bloques de tamaño predeterminado, en la etapa c) dicha serie de bloques correspondientes a cada imagen se convierten, cada uno, en una cadena de caracteres, que da lugar a una cadena de caracteres por imagen y en la etapa d) solamente se encriptan cadenas de caracteres correspondientes a imágenes con al menos un píxel no blanco.

2. El método según la reivindicación 1 que comprende, además, la etapa de cifrado de una contraseña para la encriptación de dicha cadena de caracteres.

3. El método según la reivindicación 1 o 2 que comprende, además, la etapa de generar un marcador (200).

4. El método según cualquiera de las reivindicaciones precedentes que comprende, además, la etapa de proporcionar una opción entre una transmisión asegurada de facsimil y una transmisión no asegurada d facsimil.

5. El método según cualquiera de las reivindicaciones precedentes que comprende, además, la etapa de recibir una imagen aleatorizada, en donde dicha imagen aleatorizada recibida se almacena en una memoria asignada (42), siendo dicha imagen aleatorizada recibida expandida en una cadena de caracteres, se realiza la desencriptación de dicha cadena de caracteres y la cadena de caracteres desencriptada se convierte en una imagen de un documento.

6. El método según la reivindicación 5, en donde se solicita una contraseña de un usuario y se comprueba antes de la expansión de dicha imagen aleatorizada recibida en una cadena de caracteres.

7. Un aparato para proporcionar una transmisión asegurada de facsimil de un documento, que comprende un dispositivo de transmisión (11) para transmitir un facsimil de un documento, comprendiendo dicho dispositivo de transmisión (11) medios de generación de imágenes (12) para generar al menos una imagen de dicho documento, una unidad de encriptación (39) para generar una cadena de caracteres encriptada y medios de compresión (14) para comprimir dicha cadena de caracteres generada, después de convertirla a pixels, para crear una imagen aleatorizada a transmitirse, en donde dicha unidad de encriptación (39) tiene una memoria (42) para almacenar dicha al menos una imagen, medios de conversión para la lectura de los pixels de dicha al menos una imagen en una serie de bloques de tamaño predeterminado y para convertir dicha serie de bloques en la cadena de caracteres basándose en una tabla de conversión y medios de encriptación (40) para encriptar dicha cadena de caracteres para crear una cadena de caracteres encriptada,

caracterizado porque dichos medios de encriptación (40) están adaptados para permitir la selección entre un modo de encriptación estándar, en donde se genera una sola imagen a partir del documento completo por los medios de generación de imágenes (12) y un modo de encriptación optimizado en donde se genera una serie de imágenes por los medios de generación de imágenes (12) correspondiendo cada imagen a una sola línea del documento, siendo los pixels de cada imagen de dicha serie de imágenes leídos en una serie de bloques de tamaño predeterminado y dichas series de bloques correspondientes a cada imagen se convierten cada una en una cadena de caracteres por los medios de conversión, dando lugar a una sola cadena de caracteres por imagen y solamente las cadenas de caracteres correspondientes a imágenes con al menos un píxel no blanco son encriptadas por los medios de encriptación (40).

8. El aparato según la reivindicación 7, en donde dicho dispositivo de transmisión (11) comprende, además, una unidad central de control (22), en particular una unidad central de procesos.

9. El aparato según la reivindicación 7 u 8 que comprende, además, un dispositivo de recepción (11) para recibir un facsimil de un documento, comprendiendo dicho dispositivo de recepción (11) una memoria (42) para almacenar una imagen aleatorizada recibida, medios de expansión (14) para expandir dicha imagen aleatorizada recibida en una cadena de caracteres, medios de desencriptación (40) para desencriptar dicha cadena de caracteres, medios de conversión para convertir la cadena de caracteres desencriptada en una imagen del documento y medios de impresión (28) para imprimir dicha imagen del documento.

10. El aparato según la reivindicación 9, en donde dicho dispositivo de recepción (11) comprende, además, una unidad central de control (22), en particular, una unidad central de procesos.

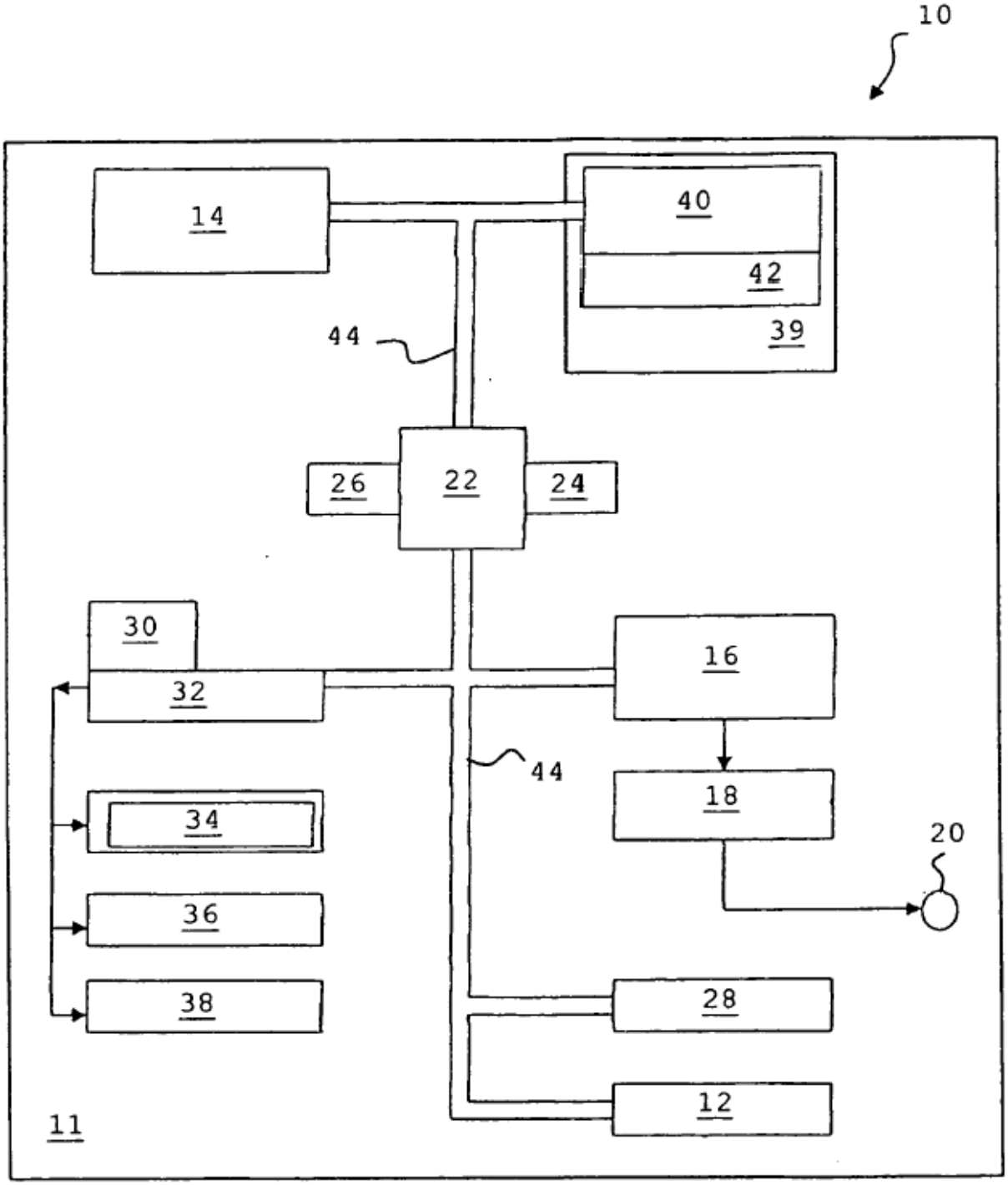

Figura 1

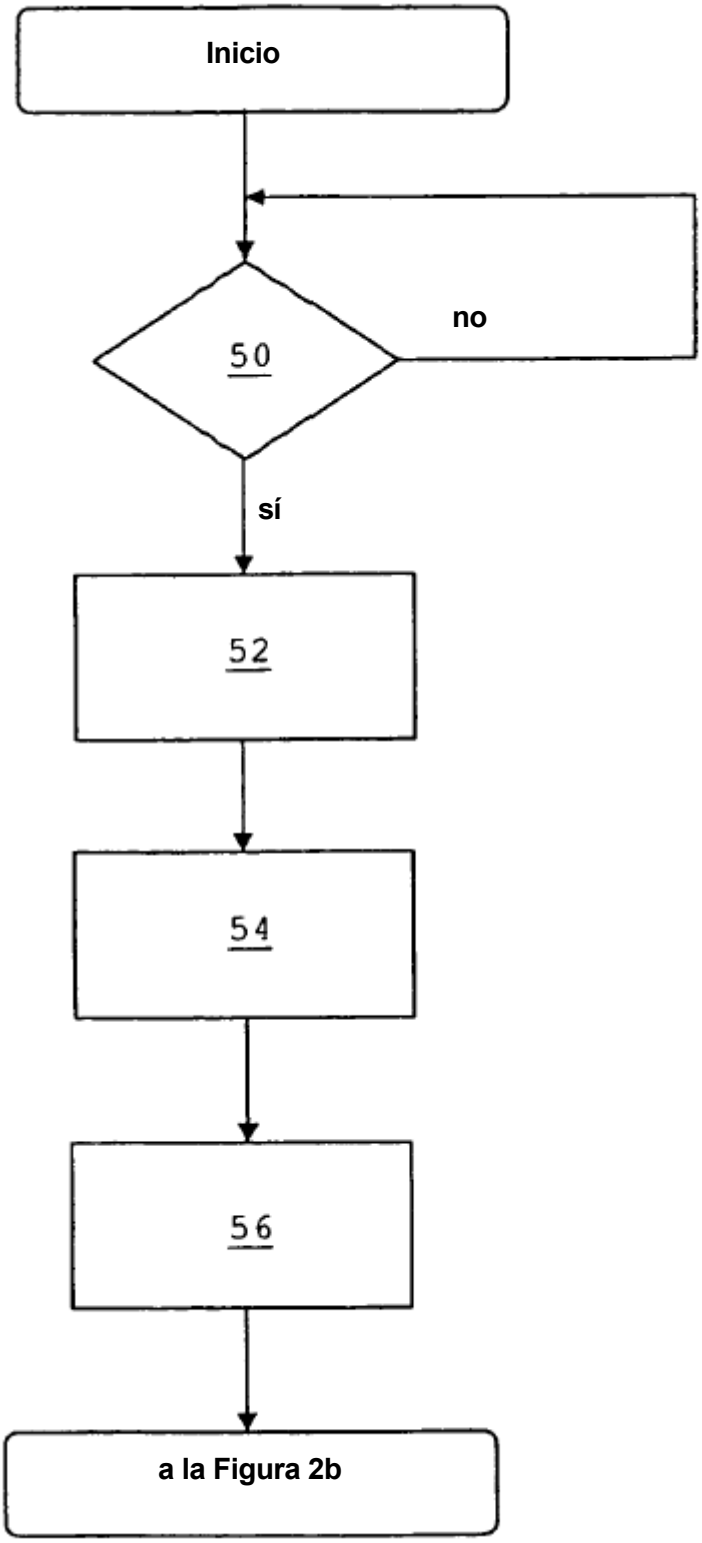

Figura 2a

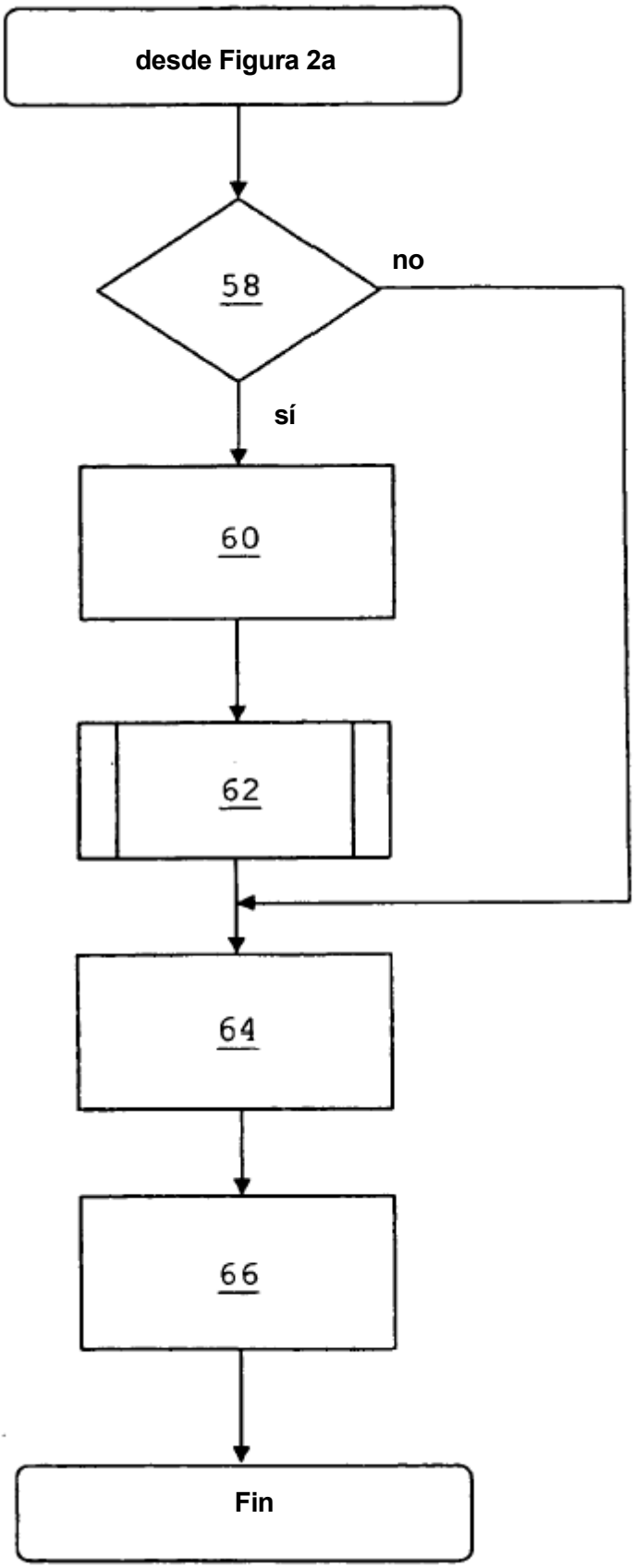

Figura 2b

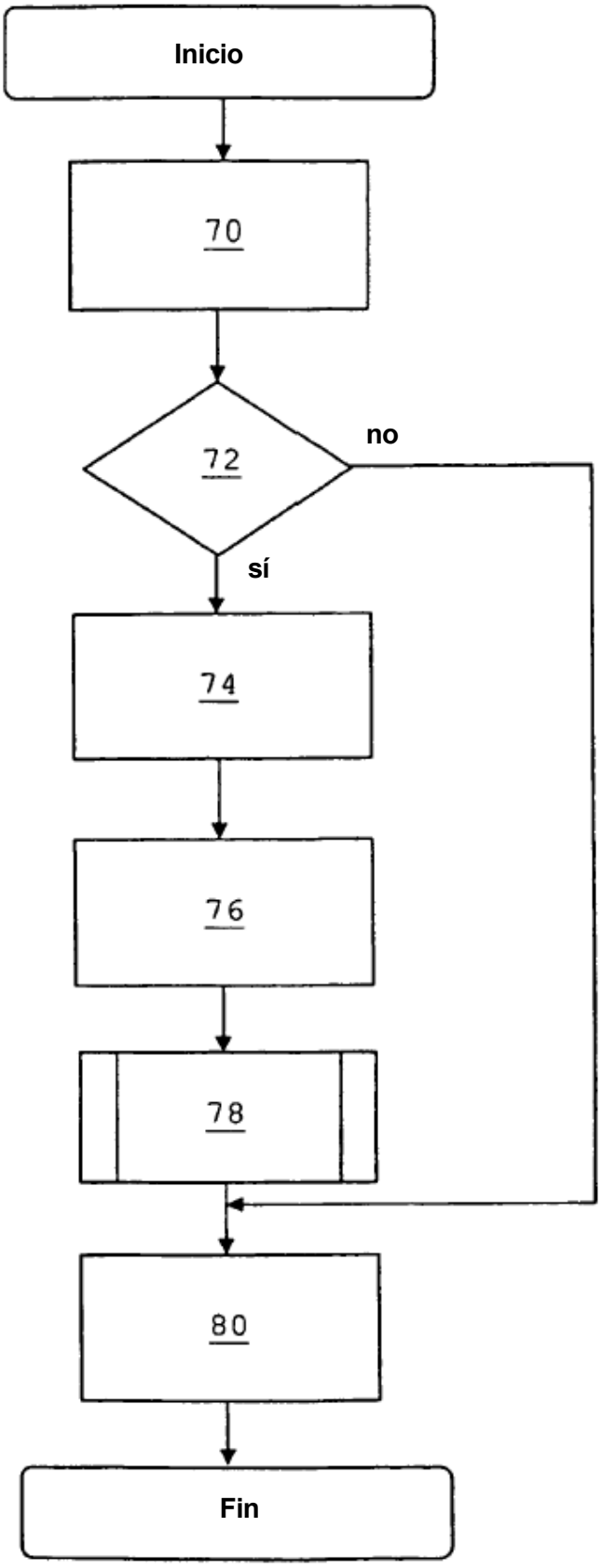

Figura 3

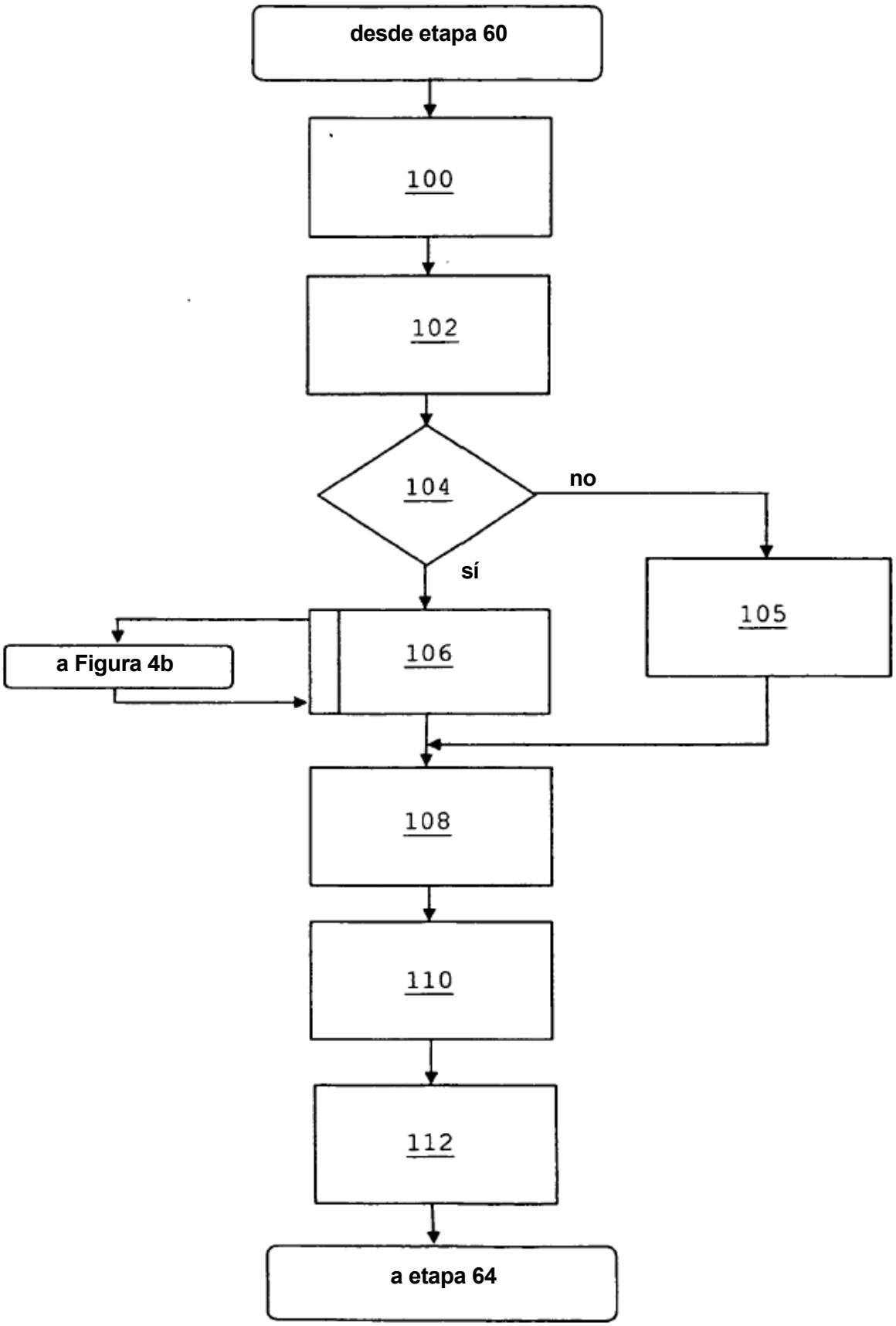
desde etapa 60
100
102
104
no
sí
105
a Figura 4b
106
108
110
112
a etapa 64

Figura 4a

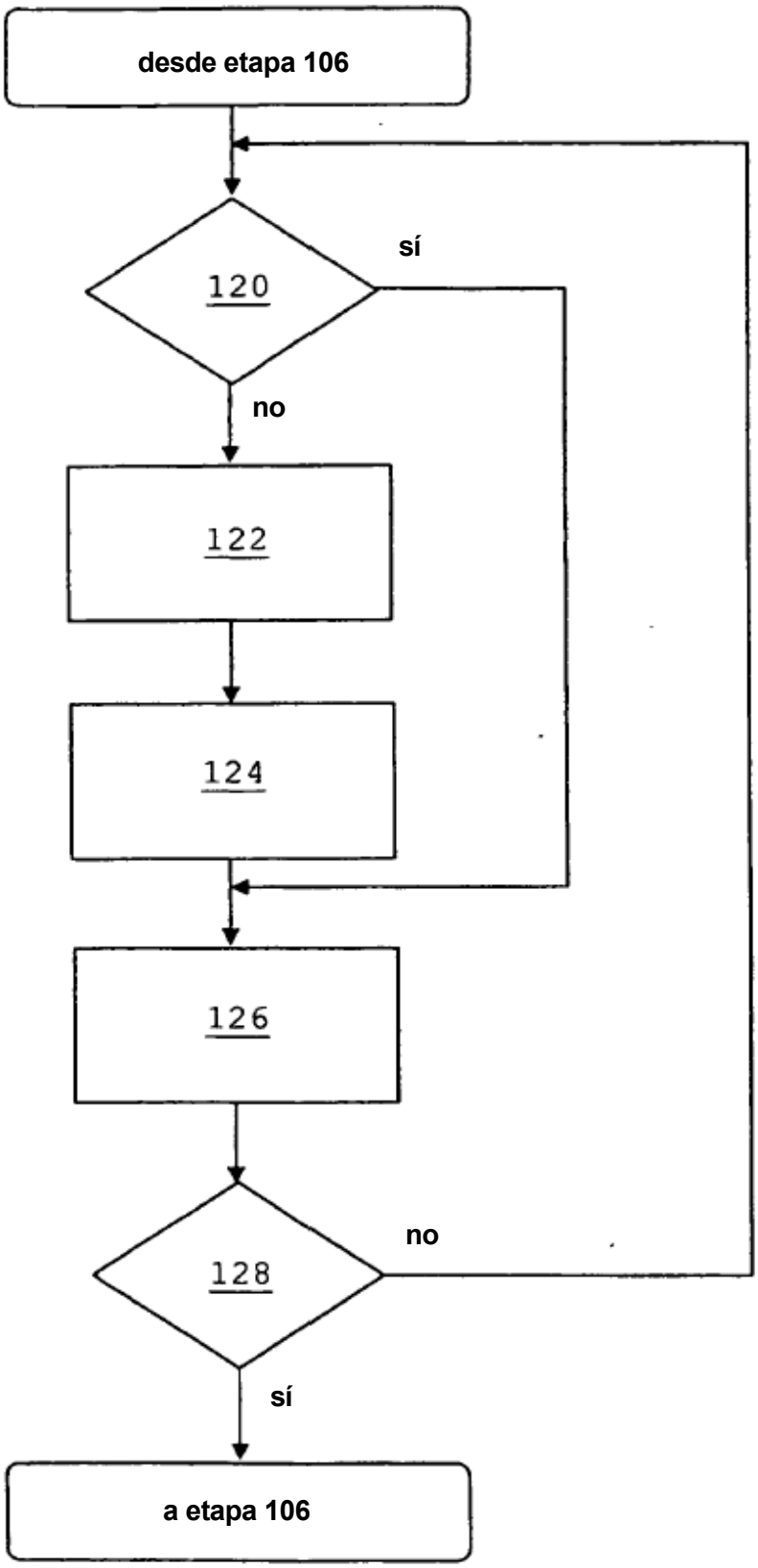

Figura 4b

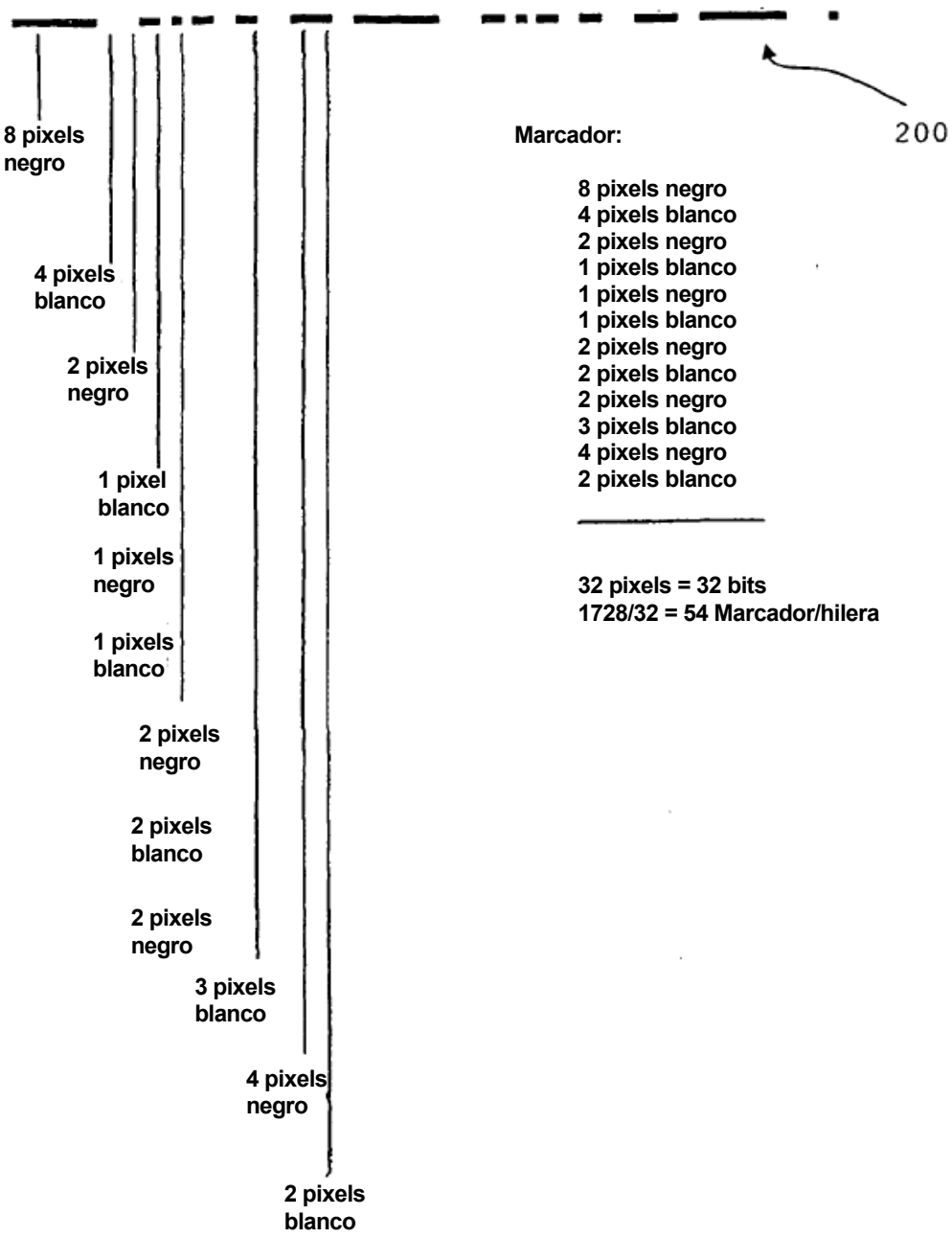
8 pixels negro
4 pixels blanco
2 pixels negro
1 pixel blanco
1 pixels negro
1 pixels blanco
2 pixels negro
2 pixels blanco
2 pixels negro
3 pixels blanco
4 pixels negro
2 pixels blanco
Marcador:
200
8 pixels negro
4 pixels blanco
2 pixels negro
1 pixels blanco
1 pixels negro
1 pixels blanco
2 pixels negro
2 pixels blanco
2 pixels negro
3 pixels blanco
4 pixels negro
2 pixels blanco
32 pixels = 32 bits
1728/32 = 54 Marcador/hilera

Figura 5

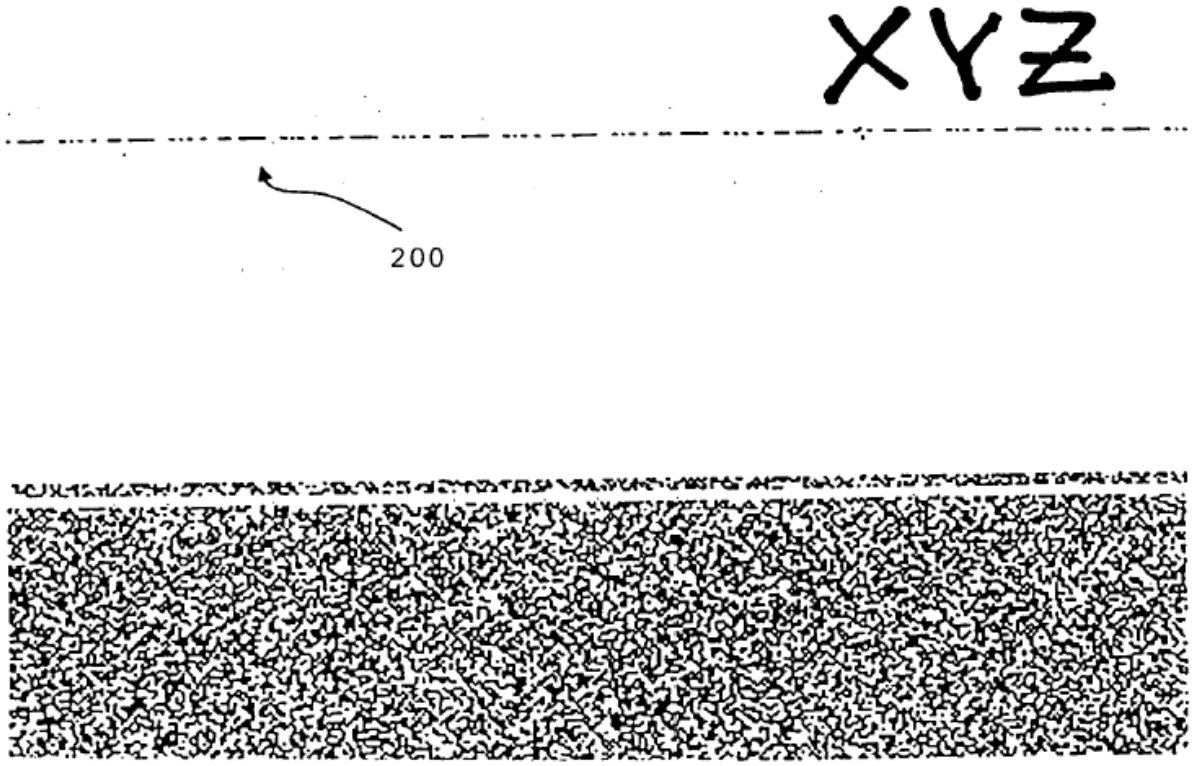

Figura 6

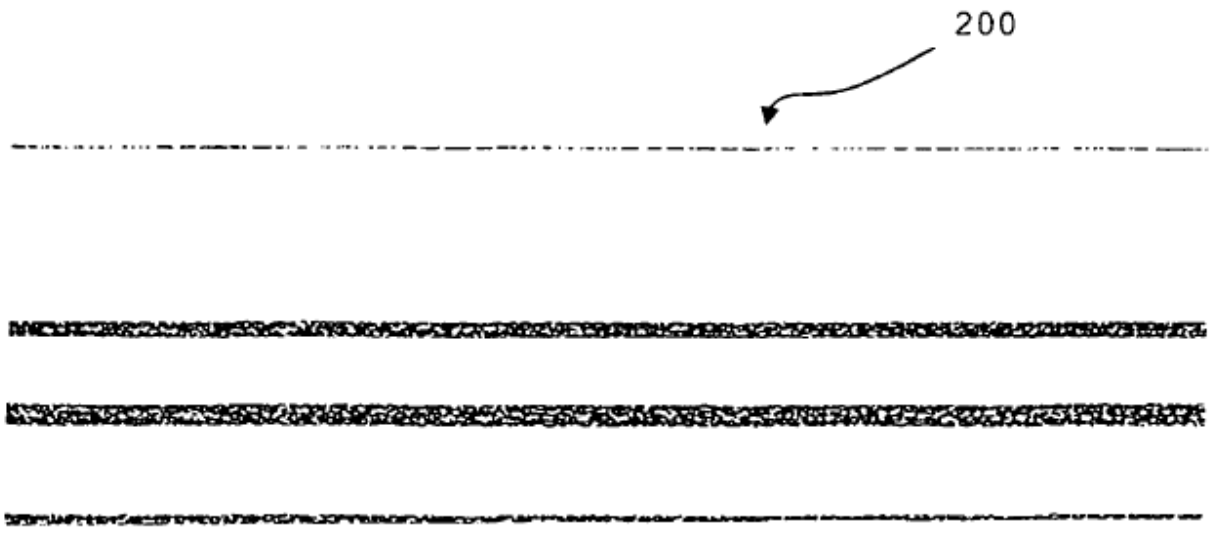

Figura 7

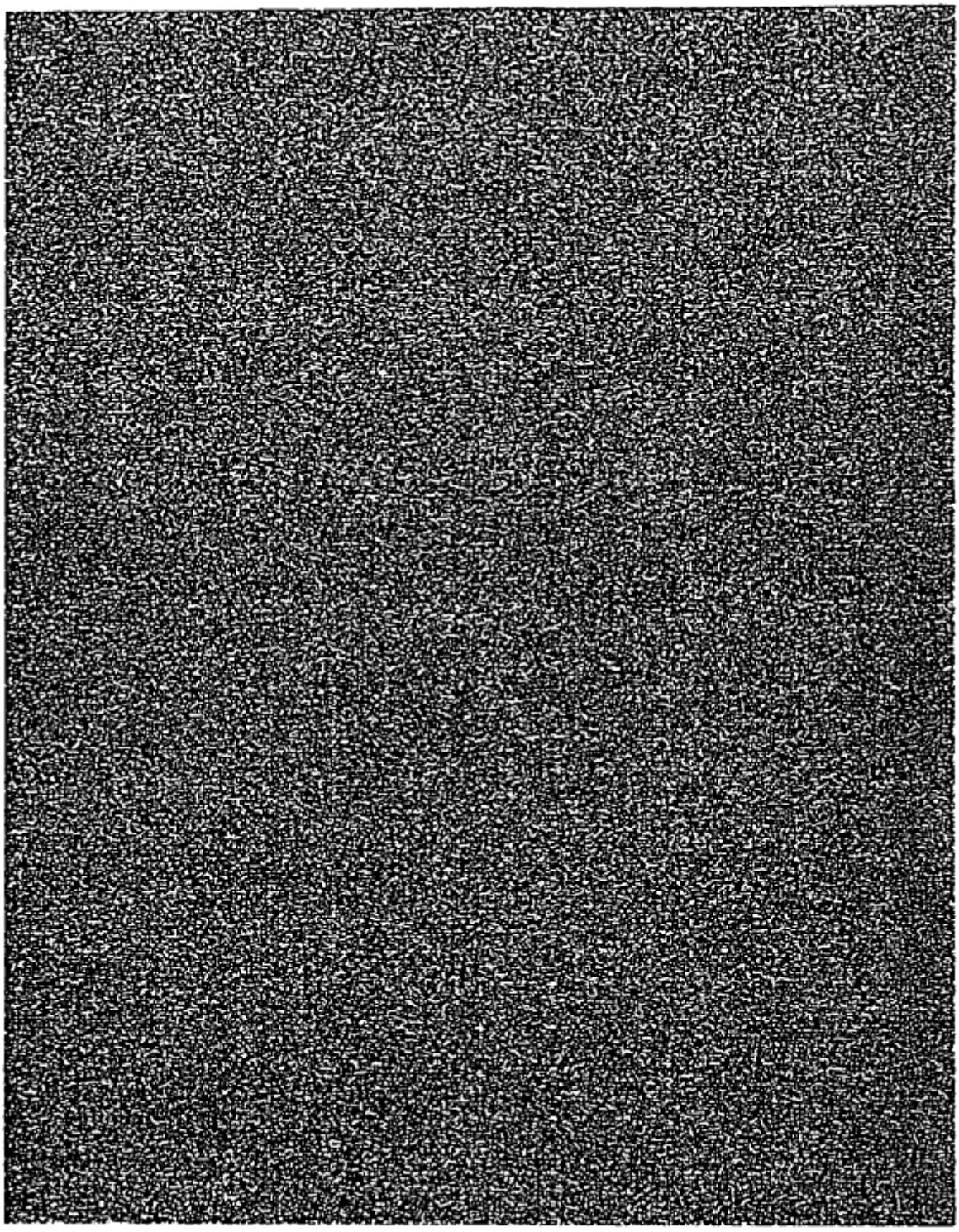

Figura 8