MINISTERIO DE INDUSTRIA
REGISTRO DE LA PROPIEDAD INDUSTRIAL

ESPAÑA

(19) ES (11) (21) 458856 (10) A1

(22) FECHA DE PRESENTACION 17 MAY. 1977

27 ENE. 1978

PATENTE DE INVENCION

(30) PRIORIDADES: (31) NUMERO	(32) FECHA	(33) PAIS
6893/76	1 Junio 1.976	Suiza

(47) FECHA DE PUBLICIDAD	(51) CLASIFICACION INTERNACIONAL	(62) PATENTE DE LA QUE ES DIVISIONARIA
	H04K	

(54) TITULO DE LA INVENCION

"PROCEDIMIENTO CON SU CORRESPONDIENTE DISPOSITIVO PARA CIFRAR Y DESCIFRAR, RESPECTIVAMENTE, INFORMACION SONORA".

(71) SOLICITANTE (S)

ANSTALT EUROPÄISCHE HANDELSGESELLSCHAFT

DOMICILIO DEL SOLICITANTE

VADUZ (Principado de Liechtenstein).

(72) INVENTOR (ES)

Peter Frutiger

(73) TITULAR (ES)

(74) REPRESENTANTE

JOSE LOPEZ CORTES

UNE A-4 MOD. 3106

UTILICESE COMO PRIMERA PAGINA DE LA MEMORIA

MEMORIA DESCRIPTIVA

El presente invento se refiere a un procedimiento para cifrar y descifrar, respectivamente, información sonora que está repartida en el eje de tiempo, en bloques parciales, que son intercambiados entre sí según una información clave, estando repartidas las señales sonoras análogas entrantes, en varias bandas de frecuencia, de las que cada una determina un canal de información, así como un dispositivo para la ejecución de este procedimiento con, por lo menos, un paso de banda bidireccional, del lado de entrada, para repartir las señales sonoras análogas entrantes en varias bandas de frecuencia, determinando cada una un canal de información.

Los procedimientos y aparatos conocidos para el cifrado lingüistico se subdividen, en lo esencial, en dos grupos:

En un grupo las señales lingüisticas análogas se transforman en señales digitales, y ello, por ejemplo, por medio de un Vocoder (Voice coder), de un sistema de modulación pulso- clave ó de un sistema de modulación Delta. Los impulsos son enlazados de manera conocida por medio de impulsos clave que son producidos por un generador de clave. Los signos cifrados de tal manera son transmitidos al lado de recepción y allí son transformados otra vez de manera correspondiente en señales lingüisticas análogas no cifradas.

Este grupo ofrece la ventaja de una alta calidad de sonido y de una elevada redundancia de la información transcrita. Además, caben tantas posibilidades de variación en el

.../...

cifrado, que es grande la seguridad contra el descifrado por no autorizados.

Sin embargo, tiene como desventaja la necesaria anchura de banda grande para la transcripción, y la sensibilidad a las distorsiones de fase en el sistema de transmisión.

En el otro grupo no se efectúa ninguna transformación de las señales lingüisticas análogas en señales digitales. La información lingüistica se reparte en grupos parciales en el eje de frecuencia y/ó de tiempo. Estos grupos parciales se permutan entonces por medio de una información clave, que es producida por un generador clave, de modo que se origina una nueva sucesión de grupos parciales. Pero la información como tal está alojada aun en la misma gama de frecuencias y de la misma clase, como la información lingüistica - original. Por ello, pueden emplearse para la transcripción de la información, sin desventaja, sistemas de transmisión, para la transcripción lingüistica con una anchura de banda correspondientemente limitada.

De ello resultan las ventajas de que no son necesarias para la transcripción de información, anchuras de banda extremadamente grandes, y que prácticamente no tienen ninguna influencia en la calidad de la información transcrita las distorsiones de fase en el sistema de transmisión.

Sin embargo, este segundo grupo presenta la desventaja de que las posibilidades de variación para permutar los grupos parciales son relativamente limitadas, de modo que - apenas es posible una seguridad eficaz contra el conocimiento de la información no cifrada por terceras personas no autorizadas.

.../...

El presente invento tiene ahora por finalidad eliminar las desventajas citadas en último lugar.

Por tanto, se presenta la tarea de crear un procedimiento ó un dispositivo, respectivamente para cifrar ó descifrar información de sonido, en particular de información lingüistica, que hacen dar una gran seguridad contra el descifrado por no autorizados, sin que sean necesarios para la transcripción de información canales de transmisión con anchuras de banda que sean esencialmente mayores que las anchuras de banda necesarias para la transcripción de la información lingüistica.

Esta tarea se resuelve con el procedimiento arriba mencionado, de acuerdo con el invento, porque las señales sonoras análogas de cada canal de información se transforman en señales digitales que, en el eje de tiempo, son subdivididas en bloques principales; porque los bloques principales de igual tiempo de cada canal de información son repartidos en subsectores, temporalmente iguales, que son cambiados según una información clave con subsectores del mismo bloque principal ó con subsectores de un bloque principal de igual tiempo de otro canal de información, y porque, después del cambio, se efectúa en cada canal de información una transformación de las señales digitales en señales análogas y una combinación de los subsectores cambiados para nuevos bloques principales, para hacer posible una elaboración posterior de los nuevos bloques principales de igual tiempo de cada canal de información.

El dispositivo para la realización de este procedi

.../...

miento se caracteriza de acuerdo con el invento por un convertidor digital análogo acoplado posteriormente al paso banda bidireccional en cada canal de información para la transformación de las señales sonoras análogas en señales digitales; por un circuito de memoria que acumula las series de impulsos de los convertidores digitales análogos que subdivide las series de impulsos acumulados de cada canal de información en bloques principales temporales y reparte estos bloques principales en subsectores temporalmente iguales; por un generador clave cooperante con el circuito de memoria, para la producción de una información clave conducida al circuito de memoria, presentando el circuito de memoria una disposición de conexión que efectúa un cambio de los subsectores de cada bloque principal, con subsectores del mismo bloque principal ó con subsectores de un bloque principal de igual tiempo de otro canal de información según la información clave obtenida; por un convertidor digital análogo acoplado posteriormente al circuito de memoria en cada canal de información, para la transformación de las señales digitales en señales análogas esperando para la elaboración posterior a la salida de cada canal de información nuevos bloques principales de igual tiempo, formados de subgrupos cambiados.

A continuación se explicará con más detalle un ejemplo de ejecución del objeto del invento a base de los diseños. Estos muestran esquematicamente:

La fig. 1 una instalación para cifrar, transcribir y descifrar información lingüistica,

La fig. 2 un diagrama de bloque de un aparato para

.../...

cifrar ó descifrar, respectivamente, la información lingüística, y

La fig. 3 dos bloques principales de igual tiempo, de la información lingüistica subdivididos en subgrupos.

En la fig. 1 hay esquemáticamente representada, una instalación para cifrar, transcribir y descifrar información lingüistica. En el lado emisor S existe un convertidor electro-acústico -1-, por ejemplo micrófono, que transforma las ondas sonoras en tensiones de frecuencia sonora. Las señales lingüisticas análogas que aparecen a la salida del convertidor -1- son repartidas en una primera parte de conexión -2- del lado emisor, que aun se describirá más detalladamente, en dos ó más bandas de frecuencia. Las señales análogas de cada banda de frecuencia son transformadas en señales digitales, que son repartidas en el eje de tiempo en bloques principales A, B. Cada bloque principal A,B se subdivide en un número dado de subsectores temporalmente iguales. En el ejemplo de ejecución descrito se subdividen los bloques principales en cuatro subsectores 1-4. En una segunda disposición de conexión -3-, del lado emisor, que se describirá aun con más detalle, se cambian los subsectores 1-4 de los bloques principales A,B, por subsectores del mismo bloque principal y/ó por los subsectores de un bloques principal de igual tiempo de otra banda de frecuencia, efectuándose este cambio de acuerdo con una información clave producida por un generador clave. En esta segunda disposición de conexión -3- se efectúa a continuación una transformación de las señales digitales de los subsectores cambiados en señales análogas y una composición de los subgrupos cambiados para nuevos grupos principa-

.../...

les A', B'. Estos nuevos grupos principales A', B' son transmitidos sobre el tramo de transcripción Ü al lado receptor E.

Los bloques principales entrantes A', B' son repartidos, en una primera disposición de conexión -4- del lado receptor, en un número correspondiente de bandas de frecuencia del lado emisor -5-. Las señales análogas de cada bloque principal A', B' son transformadas, en la disposición de conexión -4-, en señales digitales que, por su parte, son repartidas en bloques principales subdivididos en subsectores. Luego son cambiados los subsectores cambiados 1-4 de los bloques principales de igual tiempo A', B', de acuerdo con una información clave que es producida por un generador clave y que corresponde a la información clave empleada en el lado emisor S, de tal forma que la sucesión de los subsectores - 1-4, de cada bloque principal A,B, corresponde otra vez a la sucesión existente originalmente en el lado emisor S. En una segúnda disposición de conexión -5-, del lado receptor, se transforman las señales digitales de los bloques principales A,B, otra vez en señales análogas, que son transformadas por medio de un convertidor electro-acústico -6-, (altavoz), otra vez en potencia acústica.

Por medio del diagrama bloque de la fig. 2 se describe a continuación el aparato del lado emisor, para cifrar la información lingüistica.

Las señales lingüisticas no cifradas análogas que entran en la entrada -21, procedentes del convertidor electro-acústico -1-, no mostrado, son repartidas por medio de un paso banda bidireccional -7-, que consiste en dos filtros -8-,

.../...

-9-, en dos bandas de frecuencia. Cada banda de frecuencia determina un canal de información I_1 ó I_2 respectivamente. Un convertidor digital análogo -10-, ú -11-, respectivamente, - está acoplado en cada canal de información I_1, I_2 posterior al paso banda bidireccional -7-, que transforma las señales análogas en señales digitales. La digitalización de la infor-mación lingüistica análoga puede efectuarse de una manera conocida, por ejemplo, según el método delta, modificado, descrito en la Patente Suiza 542 552. Las series de impulsos que aparecen a la salida del convertidor -10-, -11- son subdivididas en bloques principales A,B, ya mencionados, que se almacenan en un circuito de memoria -12-. Cada bloque principal A,B se subdivide en un número dado de subsectores A1-A4 ó B1-B4, respectivamente, temporalmente iguales, como se muestra - en la fig. 3 y como se ha mencionado ya a base de la fig. 1. Cada subsector 1-4 se forma, por ejemplo, de cinco ó siete "Bits", análogos a los grupos de 5 ó de 7, que sirven en el code telez CCITT nº 2 ó nº 5, respectivamente, para la representación de un signo.

El circuito de memoria -12- presenta una disposición de conexión, no representada con más detalle, en la que se permutan los subsectores A1-A4 ó B1-B4, respectivamente, de bloques principales de igual tiempo A y B (fig.3), con subsectores del mismo bloque principal ó con subsectores de un bloque principal del otro canal de información. Esta permutación es posible, ya que los paquetes de impulsos que forman cada uno de los subsectores son neutros de tiempo y frecuencia.

.../...

La permutación de los subsectores se efectúa a base de una información clave que es producida por un generador - clave -13-, no descrito con más detalle. La producción de esta información clave, que se altera continuamente, se realiza de una manera de por sí conocida en la criptología. Para la sincronización del circuito de memoria -12- y del generador clave -13- existe un cadenciometro -14-.

Después de permutar los subsectores A1-A4 ó B1-B4, repectivamente, los impulsos de estos subsectores son conducidos en cada canal de información I_1 ó I_2, respectivamente, a un convertidor digital análogo -15- ó -16-, respectivamente, donde se efectúa una transformación de las señales digitales en señales análogas. Esta conversión digital análoga se efectúa de la misma manera como la conversión digital análoga en los convertidores -10- y -11-.

Los subsectores reunidos para nuevos bloques principales A', B', (fig. 1), aparecen en cada canal de información I_1, I_2 como señal análoga contínua que es llevada a un paso banda de salida -17-, que es formada de dos filtros -18-, -19-. En este paso banda de salida -17- se componen las señales análogas de cada canal de información I_1, I_2. Las señales que aparecen en la salida -22-, que representan una información lingüistica cifrada, se transcriben de una manera apropiada, de por si conocida, al lado de recepción. Los bloques principales de igual tiempo A', B' son transmitidos en ello paralelamente.

El aparato antes descrito comprende las dos disposiciones de conexión -2- y -3- mostradas en la fig. 1.

.../...

El aparato mostrado en la fig. 1 puede servir correspondientemente para descifrar las señales análogas cifradas que entran por la entrada -21- correspondiendo la forma de funcionamiento al modo de funcionamiento descrito arriba. En la salida -22-, aparecen entonces descifradas las señales análogas claras, que se hacen audibles en el convertidor electroacústico -6- (fig. 1). En este caso el aparato según la fig.2 comprende las disposiciones de conexión -4- y -5-, según la fig. 1.

Para asegurar en el lado de recepción un descifrado correcto de la información lingüistica cifrada en el lado emisor, deben ser sincronizados entre sí los dos generadores clave en el lado receptor y emisor. Esta sincronización puede efectuarse de diferente manera. En la repartición descrita en varias bandas de frecuencia, es decir, por lo menos dos, es posible, por ejemplo, prever un portador de sonido entre las bandas de frecuencia. En la fig. 3 se designa este portador de sonido con -20- y se coloca a 1600 Hz entre las dos bandas de frecuencia representadas por los bloques principales A,B. Este portador de sonido se modula con pequeña variación de frecuencia. Este portador de sonido modulado de frecuencia se transcribe al lado receptor dispuesto cada vez entre dos bloques principales de igual tiempo. En esta figura 3, la flecha -23- se refiere al portador sincr. de tiempo (t) $\pm$ 33 Hz; la flecha -24- a la amplitud A y la flecha -25 a frecuencia f(Hz).

Esta modulación de frecuencia sirve, de forma conocida, para la sincronización del generador clave en el lado receptor. El portador mismo puede servir, al mismo tiempo, como frecuencia de referencia para el aparato del lado receptor y su nivel como nivel de referencia. Esto es ventajoso -

.../...

cuando la transcripción se efectúa sobre líneas inalambricas, y el aparato del lado receptor no está estabilizado de cuarzo. En información clara no tienen importancia pequeñas divergencias de frecuencia, puesto que el hombre puede reconocer aun información lingüistica considerablemente desviada en la frecuencia. Pero para aparatos clave no es verdad esto. Pero debido al portador de sonido, es posible ahora, por medio de procedimientos de sintonización de frecuencias automáticas, que en general son ya conocidos en el ámbito de alta frecuencia y se aplican ahora en el ámbito de baja frecuencia, desviar las señales que entran en el lado receptor a la posición de frecuencia correcta para el aparato receptor.

Para poder efectuar la sincronización antes descrita, el aparato dé cifrado, lado emisor, debe tener un generador de sonido para la producción del portador de sonido y un dispositivo correspondiente para la modulación de frecuencia. El aparato de descifrado receptor debe estar provisto, correspondientemente, de un dispositivo de demodulación y de un dispositivo de sintonización de frecuencia y de nivel.

El sistema descrito tiene la ventaja de que es posible un gran número de posibilidades de variación en la permutación de los subsectores. En el ejemplo de realización descrito, con dos bandas de frecuencia y cuatro subsectores por bloque principal, resultarón 8! = aproximadamente $4.x10^4$ permutaciones, que dan con el correspondiente dimensionamiento del generador clave una gran seguridad contra el descifrado por no autorizados.

Es posible repartir las señales lingüisticas entran

.../...

tes en más de dos bandas de frecuencia y/ó repartir los bloques principales de cada banda de frecuencia en más de cuatro subsectores. Con ello se aumenta considerablemente el número de las permutaciones posibles.

Un descifrado mediante correlación se dificulta mucho con la instalación descrita, ya que la información cifrada presente está formada de paquetes de impulsos que se comportan neutros en tiempo y frecuencia.

La instalación descrita no presenta ninguna parte mecánicamente movible y necesita sólo los usuales canales - lingüisticos para la transcripción de la información cifrada.

17 MAY. - 12 -

R E I V I N D I C A C I O N E S

En esta Patente de Invención se reivindica:

1.- Procedimiento con su correspondiente dispositivo para cifrar y descifrar, respectivamente, información sonora, que está repartida en el eje de tiempo en bloques parciales que, de acuerdo con una información clave son cambiados entre sí, siendo repartidas las señales sonoras análogas entrantes en varias bandas de frecuencia de las que cada una determina un canal de información, caracterizado: por las señales sonoras análogas de cada canal de información (I_1, I_2); por señales digitales que son subdivididas en el eje de tiempo en bloques principales (A,B); porque los bloques principales de igual tiempo (A,B), de cada canal de información (I_1, I_2), son repartidos en subsectores temporalmente iguales (A1-A4, B1-B4) que son cambiados de acuerdo con una información clave con subsectores del mismo bloque principal ó con subsectores de un bloque principal de igual tiempo, de otro canal de información,y porque, después del cambio se efectúa en cada canal de información (I_1, I_2) una transformación de las señales digitales en señales análogas y una composición de los subsectores cambiados para nuevos bloques principales (A', B') para hacer posible una elaboración posterior de los nuevos bloques principales de igual tiempo (A', B'), de cada canal de información.

2.- Procedimiento con su correspondiente dispositivo para cifrar y descifrar, respectivamente, información sonora, según la reivindicación 1, con por lo menos un paso - banda bidireccional del lado de entrada, para repartir las -

.../...

señales sonoras análogas entrantes en varias bandas de frecuencia, que determinan cada vez un canal de información, caracterizado por un convertidor digital análogo -10-11-, acoplado posteriormente al paso banda bidireccional -7-, en cada canal de información (I_1, I_2), para la transformación de las señales sonoras análogas en señales digitales; por un circuito de memoria -12- que acumula las series de impulsos de los convertidores digitales análogos -10-, -11- que subdivide las series de impulsos acumuladas de cada canal de información (I_1, I_2) en bloques principales de igual tiempo (A, B) y reparte estos bloques principales en subsectores temporalmente iguales (A1-A4, B1-B4); por un generador clave -13- cooperante con el circuito de memoria para la producción de una información clave conducida al circuito de memoria -12-, presentando el circuito de memoria una disposición de conexión que realiza un cambio de los subsectores de cada bloque principl (A,B), con subsectores del mismo bloque principal ó con subsectores de un bloque principal de igual tiempo de otro canal de información, según la información clave obtenida; por un convertidor digital análogo -15-, -16- acoplado posteriormente al circuito de memoria -12-, en cada canal de información (I_1, I_2), para la transformación de las señales digitales en señales análogas, esperando a la salida de cada canal de información (I_1, I_2) nuevos bloques principales de igual tiempo (A', B'), formados de subgrupos cambiados para la elaboración posterior.

3.- Procedimiento con su correspondiente dispositivo para cifrar y descifrar, respectivamente, información so-

.../...

nora, según la reivindicación 1, caracterizado porque al cifrar entre bloques principales de igual tiempo (A,B; A',B'), de dos canales de información (I_1, I_2), hay previsto un portador de tono -20-, modulado de frecuencia, que sirve al descifrar como información de sincronización y dimensión de referencia de frecuencia.

4.- Procedimiento con su correspondiente dispositivo para cifrar y descifrar, respectivamente, información sonora, según la reivindicación 2, caracterizado porque, después de los convertidores digitales análogos -15-, -16-, hay acoplado un paso banda de salida -17-, que está formado de filtros -18-, -19- dispuestos en cada canal de información (I_1, I_2) y en cuya salida (AUS) esperan las señales sonoras análogas cifradas ó descifradas respectivamente.

5.- Procedimiento con su correspondiente dispositivo para cifrar y descifrar, respectivamente, información sonora, según la reivindicación 2, caracterizado porque el paso banda bidireccional -7-, del lado de entrada, se compone de, por lo menos, dos filtros -8-, -9-, de los que cada uno está dispuesto en un canal de información (I_1, I_2).

6.- Procedimiento con su correspondiente dispositivo para cifrar y descifrar, respectivamente, información sonora, según la reivindicación 2, para cifrar información sonora, caracterizado por un generador de sonido para la producción de un portador de sonido y de un dispositivo de modulación para la modulación de frecuencia de este portador de sonido, disponiéndose el portador de sonido modulado de frecuencia entre grupos principales de igual tiempo (A,B; A',B'),

.../...

de dos canales de información (I_1, I_2) y sirviendo como información de sincronización y dimensión de referencia de frecuencia para el dispositivo a descifrar

7.- Procedimiento con su correspondiente dispositivo para cifrar y descifrar, respectivamente, información sonora, según la reivindicación 6, caracterizado porque el portador de sonido sirve de dimensión de referencia de nivel.

8.- "PROCEDIMIENTO CON SU CORRESPONDIENTE DISPOSITIVO PARA CIFRAR Y DESCIFRAR, RESPECTIVAMENTE, INFORMACION SONORA".

De conformidad en un todo en lo esencial y fines industriales a lo descrito en la precedente memoria descriptiva y gráficamente representado en los adjuntos planos para su mejor comprensión.

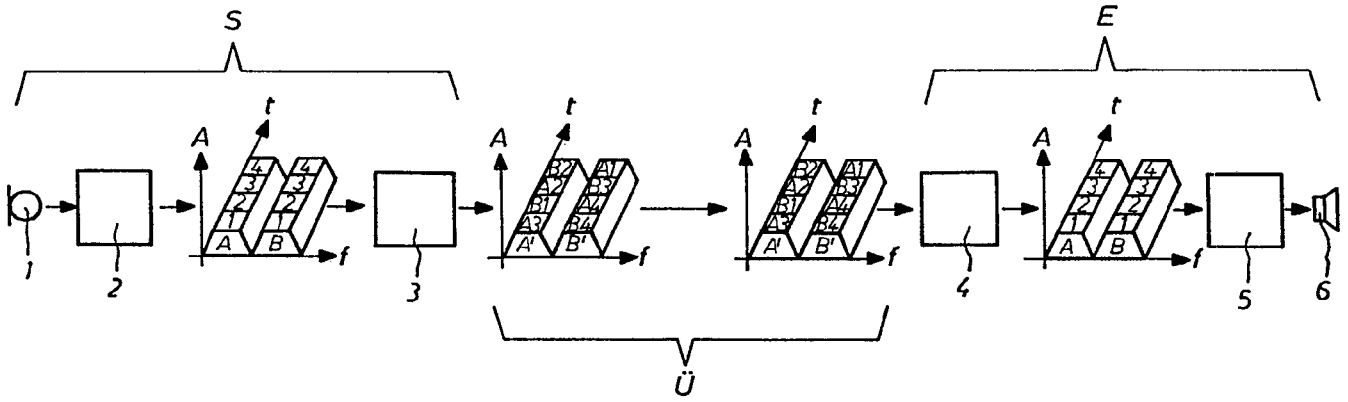
Esta memoria consta de QUINCE hojas escritas ó mecanografiadas por una sola cara a doble espacio.

Madrid. 17 MAY. 1977

Por autorización de la interesada.

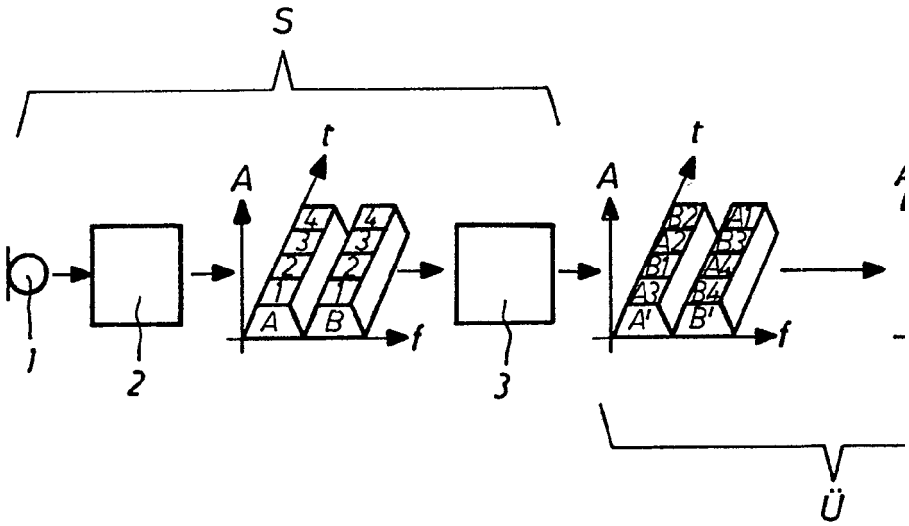
1 MAY 1977

Fig.1



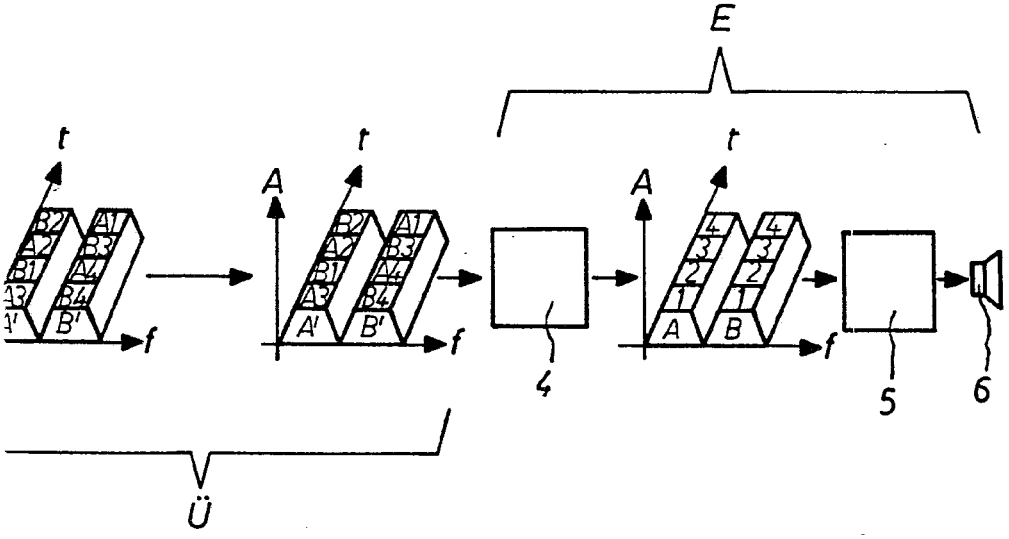
MADRID 17 MAY 1977

Fig. 1



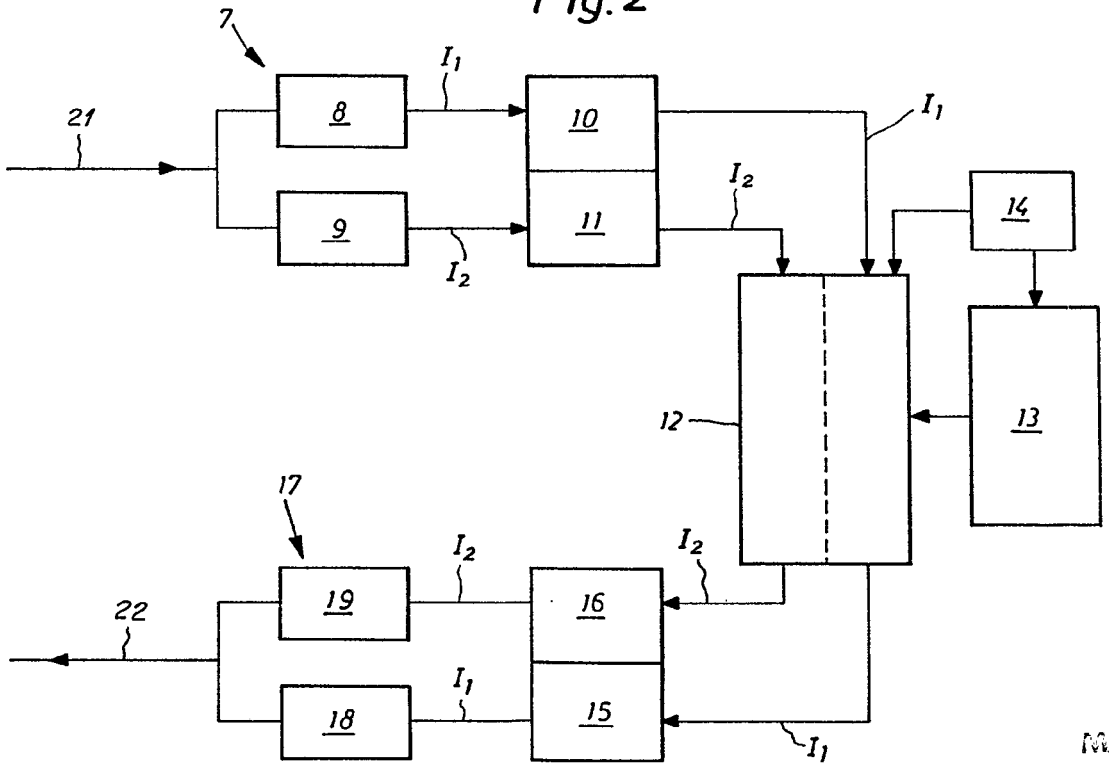
17 MAY 1977

Fig. 1



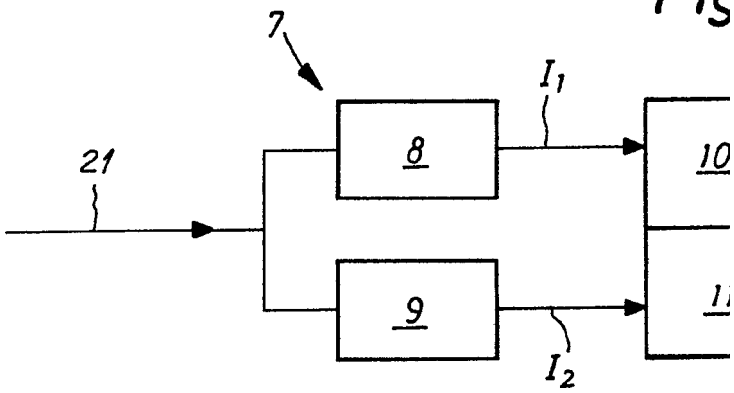
MADRID 17 MAY 1977

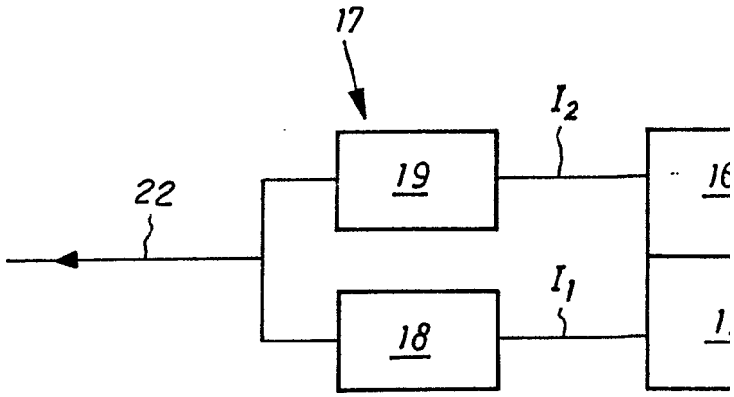
Fig. 2



MADRID 1 / MAY 1977

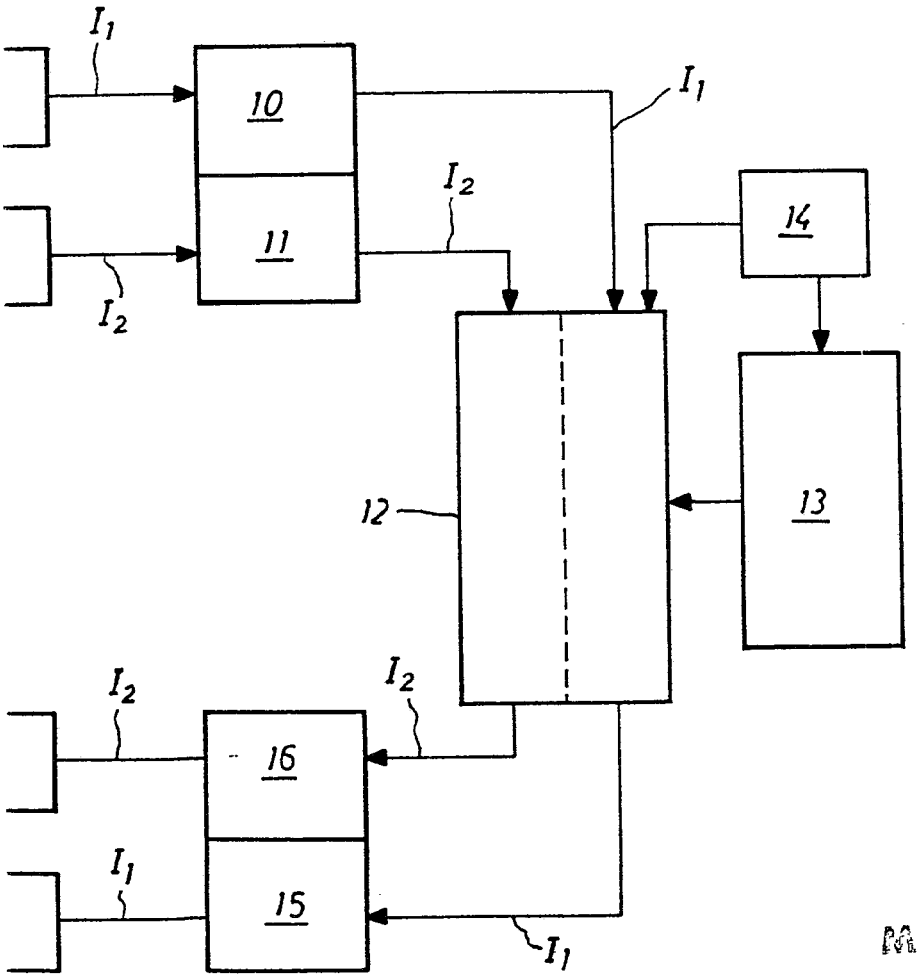
Fig





17 MAY. 1977

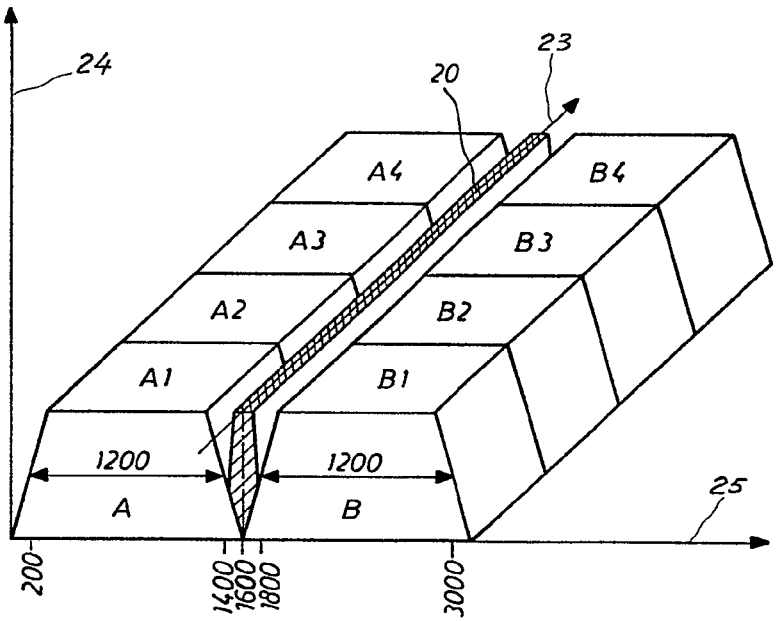
Fig. 2



MADRID 17 MAY 1977

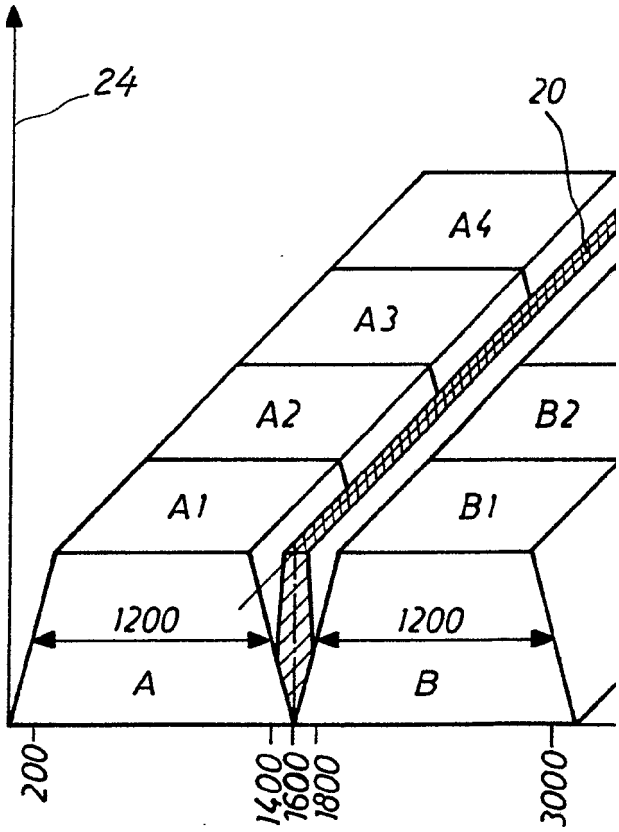
17 MAY 1977

Fig.3



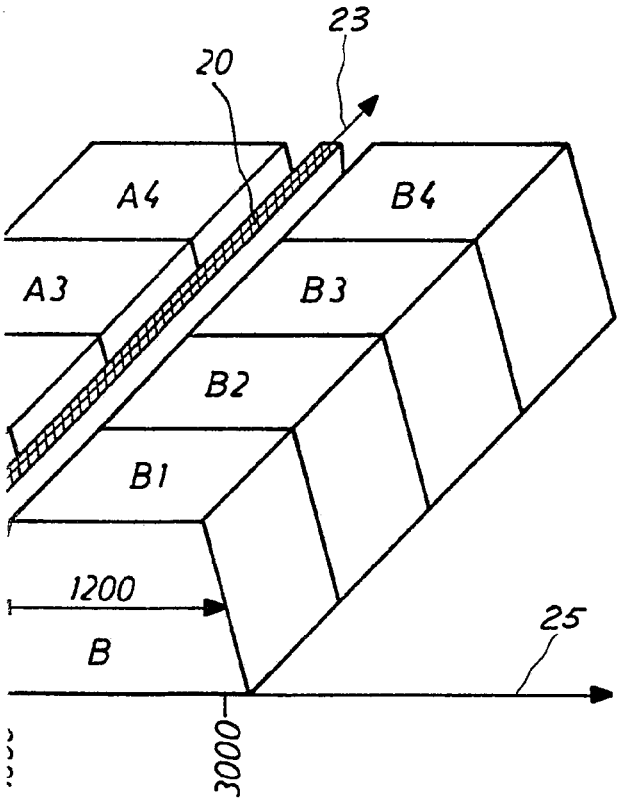
MADRID 17 MAY 1977

Fig.3



17 MAY 1977

Fig.3



MADRID 17 MAY. 1977