

①2 DEMANDE DE BREVET D'INVENTION

A1

②2 Date de dépôt : 06.01.93.

③0 Priorité :

④3 Date de la mise à disposition du public de la demande : 08.07.94 Bulletin 94/27.

⑤6 Liste des documents cités dans le rapport de recherche préliminaire : *Se reporter à la fin du présent fascicule.*

⑥0 Références à d'autres documents nationaux apparentés :

⑦1 Demandeur(s) : HULIN Gilbert — FR.

⑦2 Inventeur(s) : HULIN Gilbert.

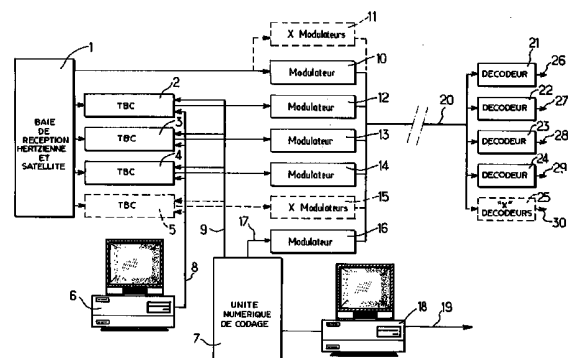
⑦3 Titulaire(s) :

⑦4 Mandataire : Cabinet Moutard.

⑤4 Procédé et dispositif pour le cryptage de canaux de télévision.

⑤7 Dans un réseau (20) de diffusion de programmes de télévision sous la forme de signaux vidéo modulés, vers une multiplicité d'abonnés, et comprenant une pluralité de canaux (11 à 16), le procédé selon l'invention consiste à utiliser un canal libre (16) comme canal de service pour transmettre, sous la forme d'un signal vidéo, à chaque décodeur (21 à 25) dont est équipé chaque abonné, des informations comprenant notamment les codes d'identification des décodeurs qui doivent s'activer, et un code d'abonnement associé à chaque code d'identification pour indiquer à chaque décodeur activé, les canaux qu'il doit décrypter.

La présente invention s'applique notamment à la diffusion de programmes de télévision payants sur les réseaux câblés.



PROCÉDÉ ET DISPOSITIF POUR LE CRYPTAGE DE CANAUX DE  
TÉLÉVISION.

La présente invention concerne un procédé de cryptage de  
5 signaux vidéo, et plus particulièrement, de signaux vidéo  
diffusés par l'intermédiaire de réseaux câblés. Elle  
concerne également le dispositif mis en oeuvre par le  
procédé.

10 Elle s'applique notamment au cryptage d'émissions de télé-  
vision dans le but d'empêcher les téléspectateurs qui n'ont  
pas souscrit à un abonnement, de recevoir de manière  
correcte ces émissions sur leur poste de télévision.

15 En général, un signal vidéo comprend des tops de  
synchronisation délimitant les signaux permettant de  
reconstituer chaque ligne de l'image, chaque image étant  
constituée de plusieurs trames, elles-mêmes constituées par  
les lignes. Chaque trame est également délimitée dans le  
20 signal vidéo par des tops de synchronisation trame composés  
par une série particulière de tops de synchronisation  
ligne. Un signal vidéo comporte également une partie

permettant de véhiculer le son qui est modulé autour d'une fréquence porteuse.

Pour être diffusé soit par voie hertzienne, soit sur un réseau câblé, un signal vidéo est modulé en amplitude  
5 autour d'une fréquence porteuse haute fréquence. Lorsque plusieurs signaux différents doivent être diffusés par le même moyen, on divise alors le spectre des fréquences disponibles en canaux, chacun étant réservé à un signal vidéo qui est modulé à l'aide d'une porteuse dont la  
10 fréquence est voisine de celle du milieu du canal.

Or, on sait qu'à l'heure actuelle, les chaînes de télévision privées, chargées de l'exploitation d'un canal de télévision, sont financées par la publicité, et certaines  
15 d'entre elles, par les téléspectateurs qui leur payent un abonnement. En contrepartie, les téléspectateurs reçoivent un décodeur qui leur permet de décrypter, et donc de recevoir parfaitement les émissions cryptées diffusées sur ce canal.

20

Les techniques de cryptage connues actuellement s'appliquent au signal vidéo avant modulation et consistent à séparer au préalable, le son et l'image pour les crypter différemment, puis à reconstituer le signal vidéo à l'aide  
25 du son et de l'image cryptés.

Ces techniques de cryptage de signaux vidéo présentent l'inconvénient majeur d'être lourds à mettre en oeuvre tant sur le plan pratique que financier.

30 En effet, elles nécessitent que chaque abonné dispose d'un décodeur distinct pour chaque canal crypté qu'il désire recevoir. Il est clair que cette solution, qui donne satisfaction lorsqu'une seule chaîne cryptée est diffusée sur un territoire par l'intermédiaire d'un réseau câblé ou  
35 par voie hertzienne, est difficilement applicable à des réseaux câblés dont les canaux seraient exploités séparément pour transmettre des programmes payants. Il est

en effet peu concevable d'imposer aux abonnés d'acquérir et d'installer chez eux plusieurs appareils décodeurs.

En outre, le prix des décodeurs de ce type est relativement élevé, et cela d'autant plus que, pour garantir une certaine inviolabilité, on a augmenté la complexité du mode de cryptage, et donc les circuits électroniques de décryptage. Cet inconvénient est renforcé par le fait qu'il occasionne un coût supplémentaire au niveau de l'abonnement qui devient dissuasif pour un grand nombre de téléspectateurs potentiels.

C'est donc une solution inapplicable sur de grandes échelles.

Par ailleurs, le type de codage utilisé, qui porte sur le signal vidéo, oblige l'utilisateur à disposer de téléviseurs et magnétoscopes spécifiquement équipés d'une prise dite péritélévision.

Toutes ces raisons ont contribué à limiter le développement des réseaux câblés et de chaînes de télévision payantes.

La présente invention a pour but de supprimer ces inconvénients. A cet effet, elle propose un procédé de cryptage d'au moins un signal vidéo émis par modulation d'une porteuse haute fréquence vers une multiplicité d'abonnés, sur un canal respectif d'un réseau qui regroupe une pluralité de canaux de diffusion de programmes de télévision, chacun des abonnés étant équipé d'un décodeur connecté à des appareils de visualisation et/ou d'enregistrement d'images vidéo, et recevant directement le signal vidéo modulé.

Ce procédé est caractérisé en ce qu'il consiste à utiliser un canal libre du réseau comme canal de service pour transmettre des informations permettant à chaque décodeur en service, de déterminer s'il doit ou non décrypter le signal vidéo et comment le faire.

Cette solution offre une grande souplesse d'utilisation tant du côté de l'abonné qui bénéficie d'un abonnement personnalisé, que du côté de l'exploitant du réseau qui peut contrôler chaque abonné directement et instantanément  
5 par l'intermédiaire du canal de service.

Ainsi, par exemple, dans le cas où un abonné n'a pas renouvelé un abonnement, l'exploitant du réseau peut télécommander le décodeur de l'abonné pour mettre hors service  
10 le décryptage du canal concerné, simplement en retirant les informations permettant d'identifier le décodeur concerné des informations transmises sur le canal de service.

Cette solution permet également à un téléspectateur de payer pour recevoir une seule émission de télévision. Dans  
15 ce cas, l'exploitant du réseau va activer le décodeur de l'abonné pour le canal concerné uniquement pendant la durée de transmission de l'émission.

Selon une particularité de l'invention, le procédé  
20 s'applique simultanément à une pluralité de canaux de diffusion de programmes de télévision, et comprend les étapes suivantes :

- l'émission cyclique d'informations sur le canal de  
25 service vers les décodeurs connectés au réseau, à savoir pour chaque décodeur :

- . un code d'identification du décodeur, chaque décodeur mémorisant un code d'identification, et
- 30 . un code d'abonnement spécifiant les canaux pour lesquels un abonnement à été souscrit par l'abonné qui détient le décodeur identifié ;

et pour chaque canal de diffusion de programmes de télévi-  
35 sion,

- la modulation d'une porteuse haute fréquence avec le signal vidéo, et le cryptage de ce dernier ; et

- l'émission du signal vidéo modulé et crypté sur le canal de diffusion ;

et pour chaque décodeur :

5

- la réception des signaux vidéo modulés émis respectivement sur chaque canal de diffusion et la réception des informations émises sur le canal de service ;

- la comparaison des codes d'identification reçus avec celui mémorisé par décodeur ;

- si l'un des codes d'identification reçus correspond à celui du décodeur, le décryptage des signaux vidéo modulés transmis respectivement par les canaux identifiés dans le code d'abonnement ; puis,

- la transmission des signaux vidéo modulés à l'appareil de visualisation et/ou d'enregistrement de l'abonné.

Cette caractéristique offre de nombreux avantages.

En particulier, elle permet le décryptage simultané de plusieurs canaux, avec un seul décodeur.

En outre, comme le décryptage est effectué par le décodeur directement sur le signal modulé reçu par l'abonné, il n'est pas nécessaire d'utiliser des téléviseurs et des magnétoscopes spécialement équipés de prises destinées à la connexion d'un décodeur.

Par ailleurs, le décryptage, qui s'applique directement sur le signal vidéo modulé, est relativement simple à mettre en oeuvre, car il ne traite pas le son et l'image de manière indépendante, tout en offrant une inviolabilité suffisante. Celui-ci peut donc être réalisé à l'aide d'un décodeur présentant un coût relativement bas, et ce d'autant plus, que le faible coût de l'abonnement qui en résulte, constitue une bien meilleure protection contre le piratage éventuel.

Cette caractéristique offre également une grande souplesse en ce qui concerne notamment le mode de cryptage, qui peut consister, par exemple, à supprimer les tops de synchronisation du signal vidéo émis, et à les transmettre sur le canal de service. Le décryptage consiste alors simplement à recombinaison le signal de synchronisation avec le signal vidéo modulé.

Avantageusement, les signaux de service peuvent comprendre également un code de cryptage indiquant le mode de cryptage utilisé pour chaque canal.

Grâce à cette disposition, chaque canal d'un réseau câblé peut présenter un mode de cryptage différent, qui peut alors consister à décaler la porteuse du signal vidéo transmis pour un certain nombre de lignes dans l'image, l'indication des numéros des lignes décalées figurant dans le code du cryptage.

La présente invention concerne également un dispositif pour la mise en oeuvre du procédé comprenant, du côté émission, des moyens pour générer un signal vidéo à partir des informations concernant chaque abonné et pour émettre ce signal sur le canal de service, et des moyens pour crypter des signaux vidéo et pour les émettre sous forme modulée, respectivement sur d'autres canaux du réseau, et du côté réception, un décodeur par abonné, connecté entre le réseau et un appareil de visualisation et/ou d'enregistrement d'images vidéo, ledit décodeur comprenant des moyens pour recevoir et mettre en forme les informations transmises par le canal de service, des moyens pour mémoriser de manière non volatile un code d'identification et pour le comparer avec les informations reçues, et des moyens pour recevoir les signaux vidéo modulés, et pour les décrypter si le code d'identification se trouve parmi les informations reçues.

35

Quelque soit le mode de cryptage utilisé, le décodeur comporte un circuit de traitement numérique pour le canal

de service et une mémoire non volatile permettant de conserver le code d'identification du décodeur.

Un mode de réalisation du procédé et du dispositif selon l'invention sera décrit ci-après, à titre d'exemple non limitatif, avec référence aux dessins annexés dans lesquels :

10 la figure 1 représente schématiquement un diagramme synoptique du dispositif mis en oeuvre par le procédé selon l'invention ;

15 la figure 2 représente un schéma bloc d'un codeur ;

la figure 3 représente un schéma bloc d'un décodeur ;

20 la figure 4 représente schématiquement une courbe d'amplitude d'un signal vidéo en fonction du temps ;

25 la figure 5 représente schématiquement la courbe d'amplitude du signal vidéo de la figure 5 en fonction du temps après modulation en amplitude.

Sur la figure 1, les différents programmes de télévision à transmettre, par exemple, par l'intermédiaire d'un réseau câblé 20 peuvent être émis par un satellite de retransmission et reçus par une baie de réception hertzienne 1.

Les programmes que l'on désire crypter sont envoyés respectivement à des "TBC" (appareils correcteurs de base de temps) 2 à 5, qui servent, d'une part, à remettre en forme les signaux vidéo selon les normes en vigueur, 35 d'autre part, à effectuer leur cryptage, et également à garantir qu'une image est toujours présente sur chaque canal. Les signaux vidéo issus des "TBC" 2 à 5 sont

synchronisés par l'intermédiaire d'une ligne 9 de connexion à une unité numérique de codage 7, à la fois au niveau des tops de synchronisation ligne et trame.

5 Ces "TBC" 2 à 5 peuvent être également commandés par l'intermédiaire d'un micro-ordinateur 6 pour effectuer par exemple des incrustations de texte comme des sous-titrages.

10 Les signaux vidéo issus des "TBC" 2 à 5 sont envoyés aux entrées respectives de modulateurs de signaux de télévision 12 à 15.

Les autres programmes reçus par la "baie de réception hertzienne" 1 qui ne doivent pas être cryptés sont envoyés directement à d'autres modulateurs 10 et 11.

15

L'unité numérique de codage 7 sert également à mettre sous la forme d'un signal vidéo standard, des données issues d'un micro-ordinateur 18.

20 Ces données qui concernent les abonnés aux programmes cryptés, peuvent elles-mêmes être émises par un système distant sur le réseau téléphonique à destination du micro-ordinateur 18.

25 Le signal vidéo transitant sur la ligne 17 issue de l'unité numérique de codage est envoyé sur un modulateur 16 comme les autres signaux vidéo issus des "TBC" 2 à 5 ou de la baie de réception hertzienne 1.

30 Chaque modulateur 10 à 16 permet de moduler une porteuse haute fréquence avec le signal vidéo en entrée, chaque canal du réseau câblé 20 étant associé à une porteuse différente.

35 Le réseau câblé 20 permet de diffuser des programmes de télévision vers une multiplicité de téléspectateurs qui lui sont raccordés. Les téléspectateurs désirant recevoir clairement sur leur poste de télévision les programmes de télévision cryptés doivent posséder un décodeur 21 à 25 connecté directement au réseau 20, et raccordé par

l'intermédiaire d'une ligne 26 à 30 à la prise antenne de leur poste de télévision.

Certains "TBC" disponibles à l'heure actuelle sur le marché  
5 permettent, par exemple, de supprimer les tops de synchronisation ligne et trame que l'on peut trouver dans un signal vidéo. Un tel signal vidéo est inexploitable par un simple poste de télévision, car il ne peut pas fonctionner en l'absence de ces tops de synchronisation, et le télé-  
10 spectateur non équipé d'un décodeur prévu à cet effet ne pourra pas visualiser clairement les programmes dont le signal vidéo a subi un tel traitement.

Pour que de tels signaux puissent être décryptés, il est  
15 nécessaire de régénérer ces tops de synchronisation au niveau des signaux vidéo transitant sur le réseau. Pour cela, l'unité numérique de codage 7 synchronise les "TBC" pour que les signaux qui y sont issus soient parfaitement synchrones. Ainsi, le décryptage des signaux vidéo cryptés  
20 peut s'effectuer par simple recombinaison avec un seul signal de synchronisation.

Pour parvenir à ce résultat, l'unité numérique de codage 7 telle que décrite figure 2 comprend un générateur de  
25 signaux de service 31 synchronisé par le micro-ordinateur 18 par l'entrée "synchro in" 32.

Le générateur de signaux de service 31 génère les signaux synchrones suivants :

30

- un signal 37 de synchronisation ligne et trame d'un signal vidéo, c'est-à-dire, contenant uniquement les tops de synchronisation ligne et trame,

35

- un signal 9 d'impulsions périodiques pour synchroniser les "TBC" 2 à 5,

- un signal d'horloge 38 calé à la fréquence de 1,25 MHz,

- un signal "blank" synchrone du signal 37 dont le niveau correspond au niveau logique 1 sauf pendant les tops de synchronisation ligne et trame où il est au niveau  
5 logique 0.

L'unité numérique de codage 7 comprend également un port parallèle 34 du type RS 232, permettant la connexion avec le micro-ordinateur 18. Il lui permet de recevoir des mots  
10 mots de commande sur 3 bits qui peuvent être associés à des mots de données sur 8 bits.

Les mots de commande associés à une donnée sur 8 bits permettent notamment de sélectionner à l'aide d'un boîtier  
15 "CHIP SELECT" 35, l'une des mémoires tampon "ADRESS1" 42, "ADRESS2" 43, "ADRESS3" 44, "DATA1" 45, "DATA2" 45 ou "END" 46, vers laquelle la donnée associée doit être envoyée par l'intermédiaire d'un bus 41 de 8 bits.

20 Les trois premières mémoires tampon "ADRESSi" 42 à 44 permettent de sélectionner une adresse sur 17 bits d'une mémoire RAM 51 de 256 kilo-octets par l'intermédiaire d'un bus d'adresse 49 sur 17 bits également. Les deux mémoires tampon suivantes "DATAi" de 8 bits chacune permettent de  
25 constituer un mot sur 16 bits qui est ensuite transféré sur un bus de données 50 de 16 bits, vers la mémoire RAM 51 à l'adresse présente sur le bus d'adresse 49.

La mémoire tampon "END" 47 est destinée à recevoir un  
30 numéro de groupe de 256 abonnés sur 8 bits, qui est ensuite transféré dans un compteur 48, cadencé par les tops de synchronisation ligne et trame, et qui génère des mots sur 17 bits sur le bus d'adresses 49. La mémoire RAM 51 étant organisée en groupes de 256 abonnés, le compteur 48 permet  
35 d'adresser successivement, à chaque top de synchronisation ligne et trame, toutes les informations contenues dans la mémoire RAM 51, relatives aux abonnés appartenant au groupe d'abonnés indiqué dans la mémoire tampon "END" 47.

Pour cela un autre mot de commande du boîtier "CHIP SELECT" 35 permet de sélectionner le mode lecture de la RAM.

Les signaux d'horloge 38 et 39 sont combinés par une porte  
5 ET inversée 36 de manière à générer un signal d'horloge 40  
à 1,25 MHz uniquement pendant les intervalles de temps  
correspondant à la transmission des lignes du signal vidéo.  
Ce signal 40 arrive sur l'entrée horloge d'un sérialiseur  
de 16 bits "SERIAL OUT" 52 qui va convertir sous forme  
10 série à la cadence donnée par le signal 40, les données  
issues de la mémoire RAM 51 transitant sur le bus de  
données 50.

En sortie du sérialiseur 52, les données traitées sont  
15 envoyées sur la ligne 53 à destination d'un circuit  
"MATRICEUR" 33 permettant de recombinaison le signal contenant  
les données à transmettre avec le signal de synchronisation  
ligne et trame 37, afin d'obtenir un signal vidéo standard.

20 Ainsi, en fonctionnement normal, on envoie successivement,  
par le port parallèle 34, la commande "END" associée à un  
numéro de groupe de 256 abonnés pour sélectionner les  
informations du groupe d'abonnés que l'on veut émettre par  
le canal de service, suivie de la commande de passage en  
25 mode lecture. Une fois que toutes ces informations ont été  
transmises, on réitère ces opérations pour un autre groupe  
d'abonnés.

En fonctionnement de mise à jour de la mémoire RAM 51, on  
adresse successivement les 5 premières mémoires tampon 42 à  
30 46 pour y transférer une adresse et une donnée via le port  
parallèle 34, puis on sélectionne, sur le boîtier "CHIP  
SELECT" 35, un mode écriture pour commander le transfert du  
contenu des mémoires tampon "DATAi" 45 et 46 dans la  
mémoire RAM 51 à l'adresse contenue dans les mémoires  
35 tampon "ADRESSi" 42 à 44.

De cette manière, l'unité numérique de codage 7 permet de  
transmettre les données concernant les abonnés issues du

micro-ordinateur 18 sous la forme d'un signal vidéo standard.

Ces données comprennent, pour chaque abonné :

5

- un code d'identification du décodeur de l'abonné soit sur 16 bits, lorsque le nombre d'abonnés à gérer est inférieur à 64000, soit sur 32 bits ; dans ce dernier cas le nombre d'abonnés qu'il est possible de gérer est quasi-  
10 ment illimité (plus de 4 milliards) ;

- un code d'abonnement indiquant les canaux pour lesquels un abonnement à été souscrit sur 16 bits ;

15 - et éventuellement, un code de cryptage indiquant le mode de cryptage utilisé pour chaque canal.

Ces données sont transmises cycliquement sur le canal de service à raison d'une ligne par abonné, ce qui permet de  
20 transmettre les informations concernant 64000 abonnés en moins de 5 secondes (pour un signal vidéo transmettant 625 lignes par image à la cadence de 25 images par seconde).

Ces données sont reçues par le décodeur 21 à 25 de chaque  
25 abonné simultanément aux programmes de télévision transmis sur les autres canaux du réseau câblé.

Le décodeur représenté sur la figure 3 permet de reconstituer huit signaux vidéo standard à partir de signaux  
30 auxquels on a retiré les tops de synchronisation ligne et trame.

Le signal transitant sur le réseau câblé est composé de plusieurs signaux vidéo transitant chacun sur un canal  
35 distinct. Il arrive sur l'entrée 60 d'un amplificateur large bande 61 permettant de compenser l'atténuation du signal produite par le traitement réalisé par le décodeur.

Ce signal est ensuite envoyé simultanément à un tuner FI 63 et à un répartiteur 62.

Le tuner FI 63 est calé sur la fréquence porteuse du canal de service pour démoduler le signal vidéo contenant les données de service. Ce signal vidéo est ensuite envoyé à un circuit séparateur 64 permettant de générer un signal ne comportant que les tops de synchronisation 66 et un signal ne contenant que les données 67.

Le signal 66 arrive sur un générateur de signaux de service 65 du type utilisé dans l'unité numérique de codage 7 qui génère un signal de synchronisation ligne et trame 97, un signal horloge à 1,25 MHz 98, un signal "blank" 99 et un signal de synchronisation trame 100, tous ces signaux étant synchrones.

15

Le signal 67 contenant les données est envoyé sur un circuit désérialiseur 90 qui permet de reconstituer des mots de 16 bits et de les transférer sur un bus de données 91 sur 16 bits. Ce circuit est cadencé par le signal horloge 98, et est remis à zéro toutes les 16 impulsions d'horloge, en fin de constitution de chaque mot de 16 bits, par un compteur 88 également cadencé par le signal horloge 98. Bien entendu, le compteur 88 n'est activé par le signal "blank" 99 que pendant les périodes de transmission des données qui correspondent aux périodes de transmission des lignes dans un signal vidéo.

Lorsque le circuit désérialiseur 90 présente un mot de 16 bits complet sur le bus 91, le circuit 92 permet de valider l'accès à une mémoire 93 de type ROM dont le bus adresse est connecté au bus 91. Si une donnée impaire figure dans cette mémoire 93 à l'adresse présente sur le bus 91, la mémoire 93 envoie une impulsion vers une mémoire tampon 95 et vers un circuit 94.

Lorsque la mémoire tampon 95 reçoit cette impulsion, elle se met en attente du mot de 8 bits transitant sur le bus 91 qui suit le code d'identification du décodeur et qui

correspond donc au code d'abonnement, tandis que le circuit 92 invalide l'accès à la mémoire ROM 93.

Chacun des 8 bits de ce code correspond à un canal crypté et indique si le canal concerné doit être décrypté ou non.

5 Ils sont envoyés séparément sur un circuit "SWITCH SYNCHRO" 96 qui reçoit par ailleurs le signal de synchronisation ligne et trame 97 pour l'envoyer ou non sur chacune des 8 lignes d'un bus 85 en fonction de la valeur du bit correspondant du code d'abonnement.

10

De son côté, le répartiteur 62 permet de séparer les canaux non cryptés 68 des canaux cryptés, lesquels sont répartis dans huit filtres passe-bande 69 à 76 dont la fréquence centrale correspond respectivement à la fréquence de modulation des huit canaux cryptés.

15

Les huit signaux vidéo cryptés toujours sous forme modulée, sont respectivement envoyés sur huit matriceurs 77 à 84 du type utilisé dans l'unité numérique de codage 7, chacun étant relié respectivement à l'une des huit lignes du bus 85. Chaque matriceur 77 à 84 permet de recombinaison le signal vidéo modulé d'un canal avec le signal de synchronisation ligne et trame circulant éventuellement sur la ligne correspondante du bus 85.

20

25

Tous les canaux de diffusion de programmes télévision sont ensuite recombinaisonés par un circuit mélangeur 86 pour reconstituer un signal 87 unique, équivalent à celui que l'on avait en entrée du décodeur, mais parfaitement exploitable par un téléviseur ou par un magnétoscope, tous les canaux pour lesquels un abonnement a été souscrit ayant été décryptés.

30

Par ailleurs, le signal de synchronisation trame 100 arrive sur un compteur de trame 89 qui génère une impulsion toutes les 512 trames, soit environ toutes les 10 secondes. Cette impulsion est envoyée au circuit 94 pour remettre à zéro la mémoire tampon 95 si le code du décodeur n'a pas été reçu

35

pendant 10 secondes, ce qui a pour effet de commander le circuit "SWITCH SYNCHRO" 96 pour couper l'émission du signal de synchronisation ligne et trame vers les matrices 77 à 84, et donc de mettre le décodeur hors service.

5 Cette disposition permet de prendre en compte presque instantanément la fin d'un abonnement.

Le principe de cryptage utilisé par le dispositif dans l'exemple décrit précédemment, consiste donc à supprimer

10 les tops de synchronisation ligne et trame du signal vidéo. Cela revient à supprimer les impulsions négatives du signal vidéo représenté sur la figure 4, c'est-à-dire, la partie du signal située en dessous de la ligne en traits interrompus 101.

15 Une fois modulé en amplitude par modulation négative, le signal vidéo prend la forme d'un signal sinusoïdal (représenté en grisé sur la figure 5) dont la fréquence correspond à celle de la porteuse haute fréquence et dont

20 l'amplitude, qui suit la forme du signal vidéo d'origine, est maximale au niveau des tops de synchronisation.

Si l'on a auparavant retiré les tops de synchronisation ligne et trame du signal vidéo, le signal vidéo modulé ne

25 comporte que la partie du signal située entre les lignes 102 et 103 et son amplitude suit la forme du signal situé au dessus de la ligne 101 de la figure 4.

Si l'on désire crypter de cette manière un signal vidéo, il

30 suffit, par exemple, d'utiliser un "TBC" (disponible dans le commerce), capable de supprimer ainsi les tops de synchronisation ligne et trame d'un signal vidéo, et de moduler le signal ainsi obtenu. De cette manière, on obtient le signal représenté sur la figure 5, entre les

35 lignes 102 et 103, qui peut être alors envoyé sur le réseau câblé.

Par ailleurs, l'unité numérique de codage et de traitement  
7 qui synchronise tous les "TBC" 2 à 5 de manière à ce que  
tous les canaux cryptés utilisent le même signal de  
synchronisation ligne et trame, génère un signal vidéo  
5 comprenant le signal de synchronisation ligne et trame (en  
dessous de la ligne 101 sur la figure 4), et les informa-  
tions concernant chaque abonné à la place des informations  
permettant la reconstitution des lignes des images (au  
dessus de la ligne 101). Ce signal vidéo est ensuite  
10 transmis sur le canal de service du réseau câblé 20 par  
l'intermédiaire du modulateur 16.

A la réception, les matricieurs 77 à 84 vont reconstituer  
les signaux vidéo complets (figure 5) à partir du signal de  
15 synchronisation ligne et trame 97 reçu par l'intermédiaire  
du canal de service et à partir des signaux vidéo modulés  
reçus (ayant la forme du signal situé entre les lignes 102  
et 103 représenté sur la figure 5). Pour cela, il suffit  
d'étirer les enveloppes respectives des signaux vidéo  
20 modulés pendant chaque top de synchronisation.

Bien entendu, d'autres méthodes de cryptage peuvent être  
utilisées, comme par exemple, celle qui consiste à décaler  
de manière aléatoire la porteuse haute fréquence au niveau  
25 d'un certain nombre de lignes de l'image, après avoir émis  
un code de cryptage par le canal de service indiquant les  
lignes décalées.

REVENDICATIONS

1. Procédé de cryptage d'au moins un signal vidéo émis par modulation d'une porteuse haute fréquence vers une  
5 multiplicité d'abonnés sur un canal respectif d'un réseau (20) qui regroupe une pluralité de canaux de diffusion de programmes de télévision, chacun des abonnés étant équipé d'un décodeur (21 à 25) connecté à des appareils de visualisation et/ou d'enregistrement d'images vidéo, et recevant  
10 directement le signal vidéo modulé, caractérisé en ce qu'il consiste à utiliser un canal libre du réseau comme canal de service pour transmettre des informations permettant à chaque décodeur (21 à 25) de déterminer s'il doit ou non décrypter le signal vidéo et  
15 comment le faire.

2. Procédé selon la revendication 1, caractérisé en ce qu'il s'applique simultanément à une pluralité de canaux de diffusion de programmes de télévi-  
20 sion, et comprend l'émission cyclique d'informations sur le canal de service vers les décodeurs connectés au réseau, à savoir pour chaque décodeur :  
- un code d'identification du décodeur, chaque décodeur mémorisant un code d'identification, et  
25 - un code d'abonnement spécifiant les canaux pour lesquels un abonnement à été souscrit par l'abonné qui détient le décodeur identifié ;

3. Procédé selon la revendication 2, caractérisé en ce qu'il comprend pour chaque canal de  
30 diffusion de programmes de télévision :  
- la modulation de la porteuse haute fréquence avec le signal vidéo, et le cryptage de ce dernier ; et  
- l'émission du signal vidéo modulé et crypté sur le canal  
35 de diffusion ;

4. Procédé selon la revendication 3, caractérisé en ce qu'il comprend pour chaque décodeur :

- la réception des signaux vidéo modulés émis respectivement sur chaque canal de diffusion et la réception des informations émises sur le canal de service ;
- la comparaison des codes d'identification reçus avec  
5 celui mémorisé par le décodeur ;
- si l'un des codes d'identification reçus correspond à celui du décodeur, le décryptage des signaux vidéo modulés transmis respectivement par les canaux identifiés dans le code d'abonnement ; puis,
- 10 - la transmission des signaux vidéo modulés à l'appareil de visualisation et/ou d'enregistrement de l'abonné.

5. Procédé selon l'une des revendications 2 à 4, caractérisé en ce que les informations émises cycliquement  
15 sur le canal de service comprennent un code de cryptage par canal permettant aux décodeurs en service d'effectuer ledit décryptage.

6. Procédé selon l'une des revendications précédentes,  
20 caractérisé en ce que le cryptage des signaux vidéo consiste à leur supprimer des signaux de synchronisation qui permettent de reconstituer des images, ces signaux de synchronisation étant transmis par l'intermédiaire du canal  
25 de service, et en ce que le décryptage consiste à recombiner les signaux vidéo modulés avec le signal de synchronisation.

7. Procédé selon l'une des revendications précédentes,  
30 caractérisé en ce que ledit cryptage consiste à décaler un certain nombre de tops de synchronisation ligne dans une image véhiculée par signal vidéo, un code d'identification des numéros des tops de synchronisation décalés étant  
35 transmis par ailleurs par le canal de service, aux décodeurs (21 à 25) qui comprennent des moyens pour décaler en sens inverse les tops de synchronisation identifiés par ledit code.

8. Dispositif pour la mise en oeuvre du procédé selon l'une des revendications précédentes, caractérisé en ce qu'il comprend, du côté émission, des moyens pour générer (7) un signal vidéo à partir des informations concernant chaque abonné et pour émettre (16) ce signal sur le canal de service, et des moyens pour crypter (2 à 5) des signaux vidéo et pour les émettre (10 à 15) sous forme modulée, respectivement sur d'autres canaux du réseau (20), et du côté réception, un décodeur (21 à 25) par abonné connecté entre le réseau (20) et un appareil de visualisation et/ou d'enregistrement d'images vidéo, ledit décodeur (21 à 25) comprenant des moyens (63 à 65, 88, 90) pour recevoir et mettre en forme les informations transmises par le canal de service, des moyens (93) pour mémoriser de manière non volatile un code d'identification et pour le comparer avec les informations reçues, et des moyens pour recevoir (62, 69 à 76) les signaux vidéo modulés, et pour les décrypter (77 à 84) si le code d'identification se trouve parmi les informations reçues.

20

9. Dispositif selon la revendication 8, caractérisé en ce que le cryptage d'un signal vidéo est réalisé par un appareil correcteur de base de temps (2 à 5) qui supprime les tops de synchronisation ligne et trame que l'on trouve dans un signal vidéo, et en ce que les tops de synchronisation ligne et trame sont diffusés, par l'intermédiaire du canal de service, aux décodeurs qui comprennent chacun des moyens pour les recevoir (61) et les recombinaison (77 à 84) avec les signaux vidéo modulés afin d'obtenir leur décryptage.

10. Dispositif selon l'une des revendications 8 et 9, caractérisé en ce que les moyens pour générer (7) un signal vidéo à partir des informations concernant chaque abonné comprennent :

- une mémoire RAM (51) dans laquelle les informations relatives à chaque abonné sont stockées,

- des moyens pour lire (47,48) et pour mettre sous forme série (52) ces informations,
- des moyens pour générer (31) le signal de synchronisation d'un signal vidéo et pour le combiner (33) avec lesdites  
5 informations sous forme série, de manière à obtenir un signal vidéo standard.

11. Dispositif selon la revendication 10,  
caractérisé en ce que les moyens pour générer (7) un signal  
10 vidéo à partir des informations relatives aux abonnés comprennent des moyens pour mettre à jour (34, 35, 42 à 46) la mémoire RAM (51) à partir d'un micro-ordinateur (18).

12. Dispositif selon la revendication 9,  
15 caractérisé en ce que chaque décodeur comprend des moyens pour recevoir (61,63) le signal vidéo transitant par le canal de service du réseau (20), des moyens pour en extraire (64) le signal de synchronisation et les informations relatives aux abonnés, et des moyens pour mettre en forme  
20 (88,90) lesdites informations.

13. Dispositif selon l'une des revendications 9 et 12,  
caractérisé en ce que chaque décodeur comprend une mémoire  
25 tampon (95) permettant de mémoriser un code d'abonnement indiquant les canaux à décrypter, transmis à la suite du code d'identification du décodeur, et des moyens pour envoyer (96, 85), en fonction du code d'abonnement, le signal de synchronisation aux moyens pour recombinaer (77 à  
30 84) ces derniers avec les signaux vidéo à décrypter.

14. Dispositif selon la revendication 13,  
caractérisé en ce que chaque décodeur comprend des moyens pour effacer cycliquement (89, 94) le code d'abonnement de  
35 la mémoire tampon (95) si le code d'identification du décodeur n'a pas été reçu pendant un certain temps.

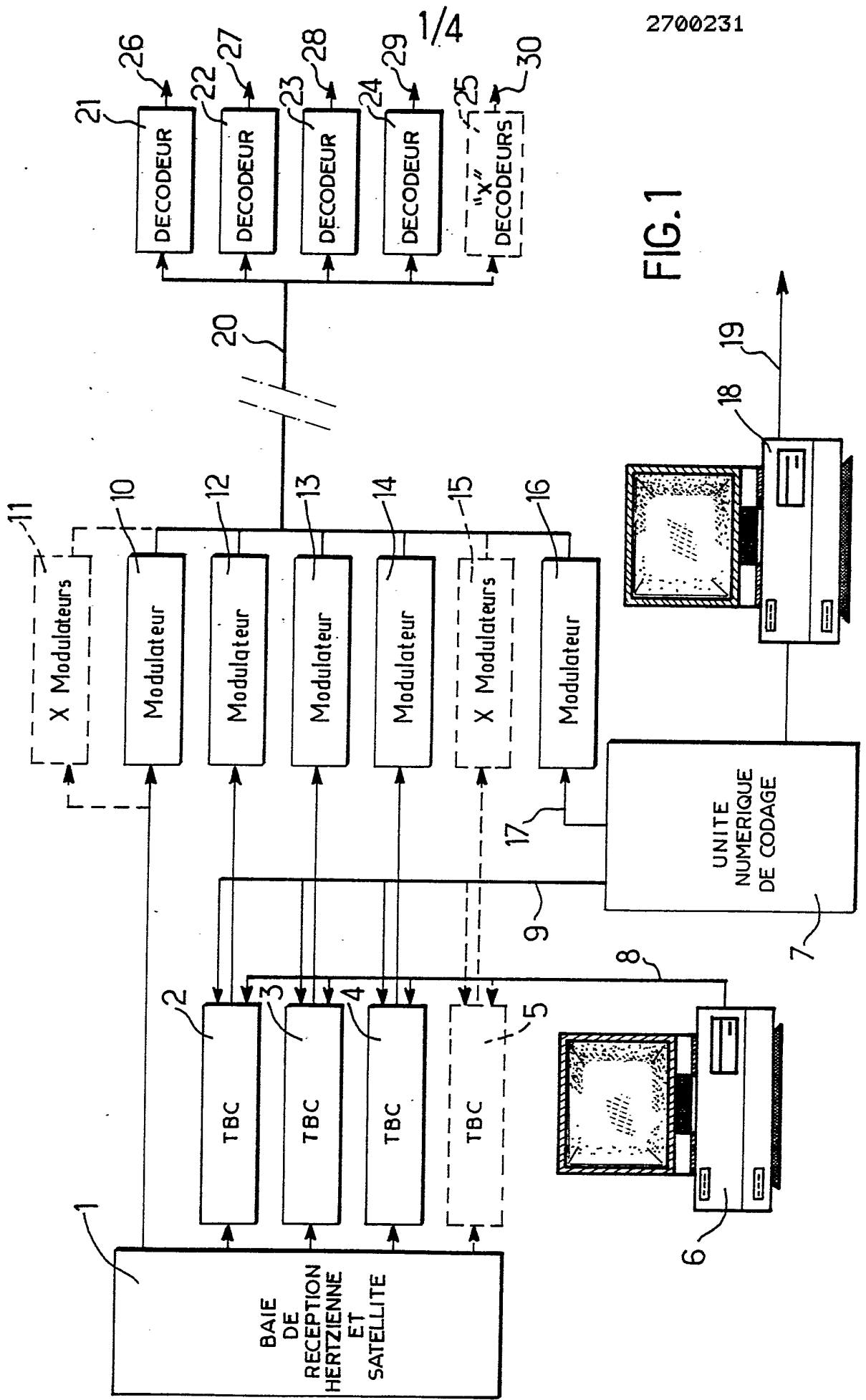


FIG. 1

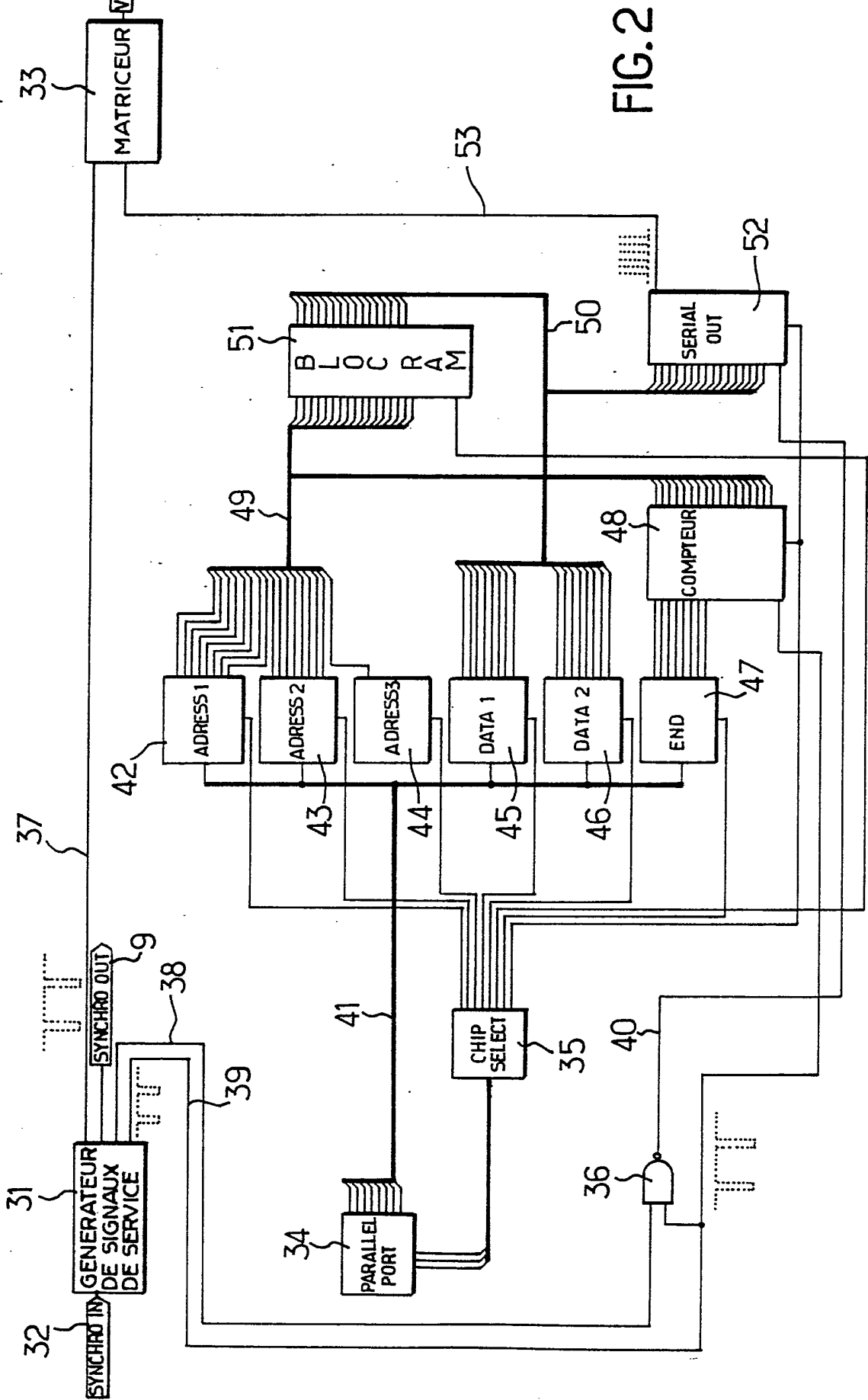


FIG. 2

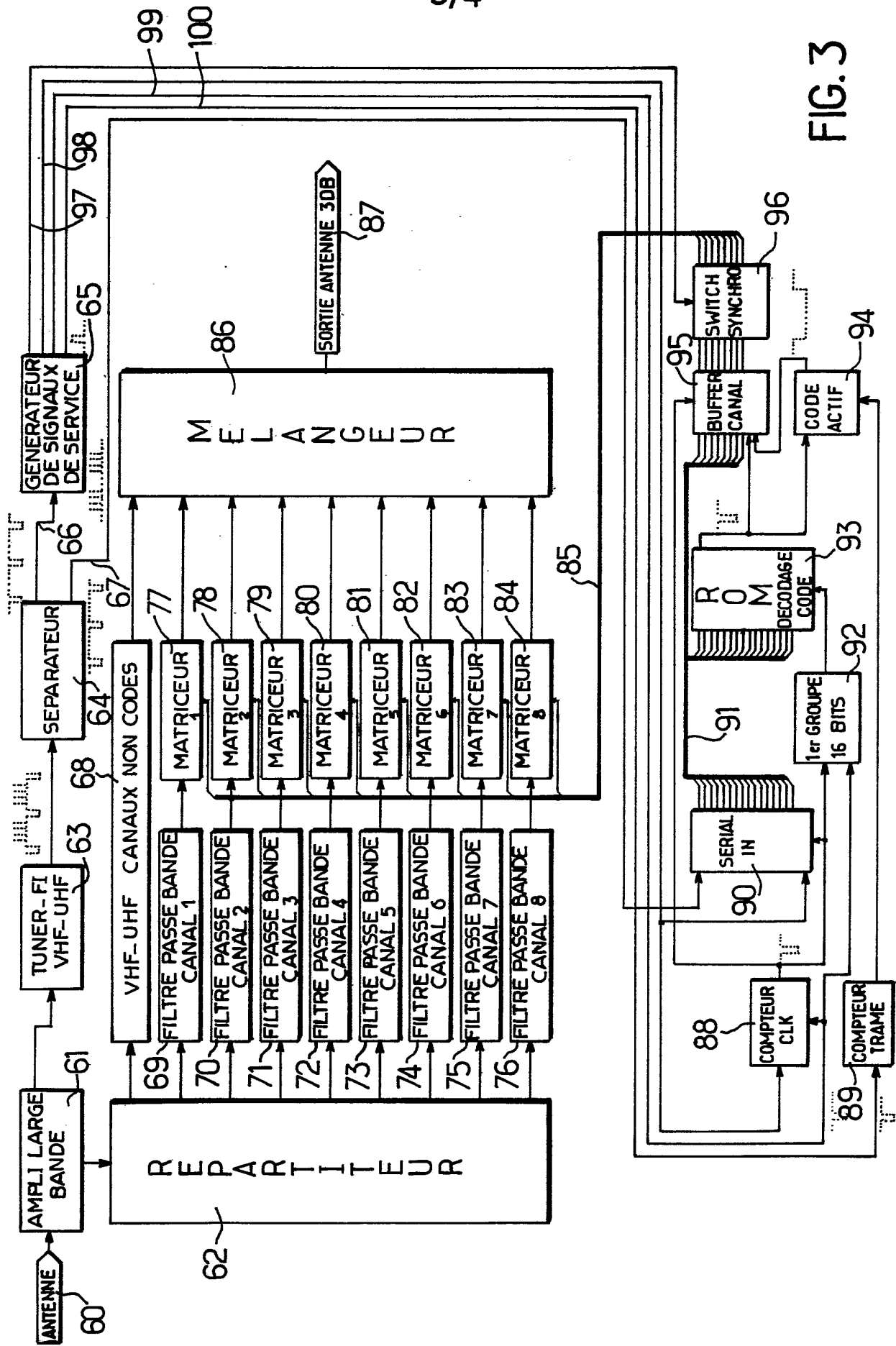


FIG. 3

4/4

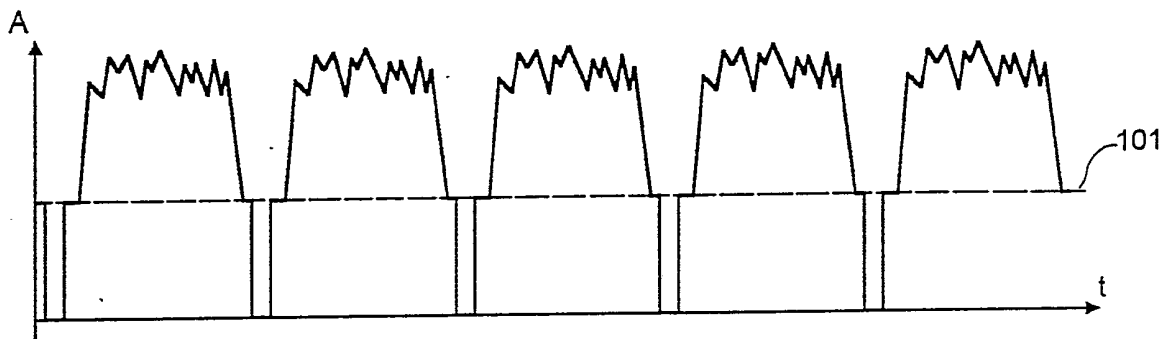


Fig. 4

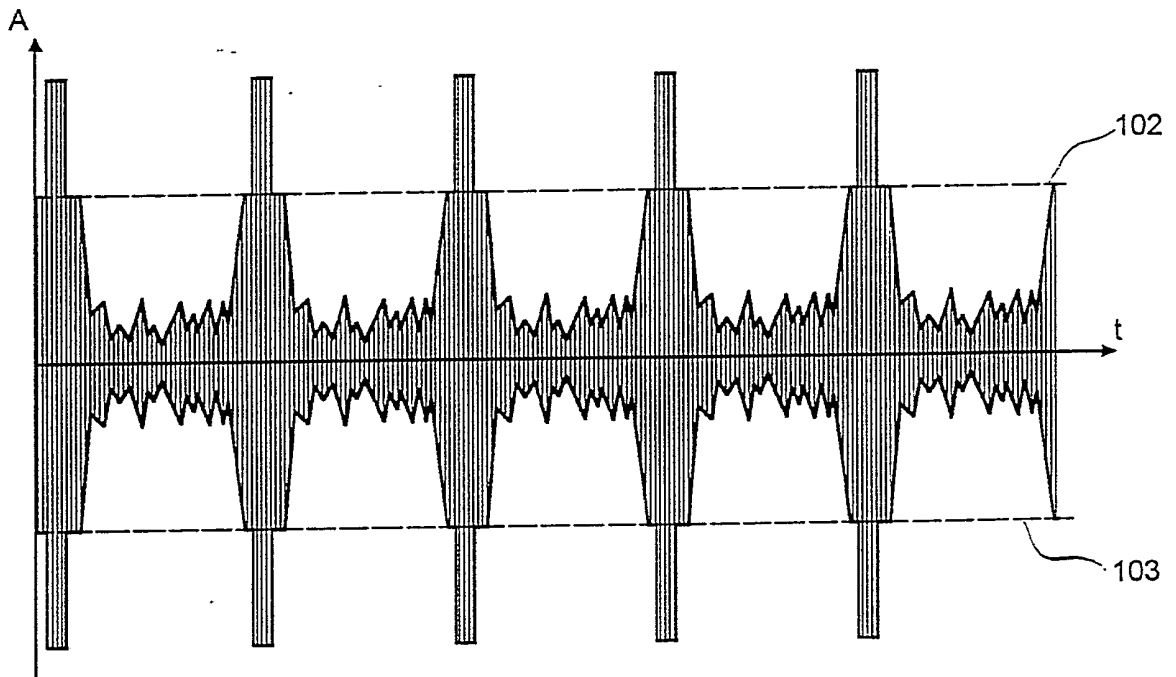


Fig. 5

INSTITUT NATIONAL

de la

PROPRIETE INDUSTRIELLE

RAPPORT DE RECHERCHE

établi sur la base des dernières revendications déposées avant le commencement de la recherche

FR 9300203

FA 483918

DOCUMENTS CONSIDERES COMME PERTINENTS		Revendications concernées de la demande examinée
Catégorie	Citation du document avec indication, en cas de besoin, des parties pertinentes	
Y	ELEKTRONIK vol. 38, no. 6, 17 Mars 1989, MÜNCHEN pages 56 - 58 , XP000039410 M.JÜNKE 'DIGITALES FERNSEHKONZEPT FÜR SATELLITEN-PAY-TV'	1
A	* le document en entier *	2-5,8, 10,11, 13,14
Y	--- US-A-4 058 830 (GUINET ET AL.) * abrégé; figure 1 * * colonne 1, ligne 28 - ligne 30 *	1
A	--- EP-A-0 161 913 (COMMUNICATION SATELLITE CORPORATION) * abrégé * * page 8, ligne 31 - page 9, ligne 20 *	1,5,8, 10,11, 13,14
A	--- US-A-5 003 592 (PIRES) * le document en entier *	1,6,7-9, 12
A	--- WO-A-9 222 987 (SCIENTIFIC-ATLANTA,INC.) * abrégé * * page 2, ligne 3 - page 3, ligne 16 *	1,6,7
A	--- US-A-4 120 003 (MITCHELL ET AL.) * colonne 1, ligne 29 - ligne 62 *	1
		-----
Date d'achèvement de la recherche		Examineur
13 JUILLET 1993		GREVE M.P.
<p><b>CATEGORIE DES DOCUMENTS CITES</b></p> <p>X : particulièrement pertinent à lui seul                      Y : particulièrement pertinent en combinaison avec un autre document de la même catégorie                      A : pertinent à l'encontre d'au moins une revendication ou arrière-plan technologique général                      O : divulgation non-écrite                      P : document intercalaire</p> <p>T : théorie ou principe à la base de l'invention                      E : document de brevet bénéficiant d'une date antérieure à la date de dépôt et qui n'a été publié qu'à cette date de dépôt ou qu'à une date postérieure.                      D : cité dans la demande                      L : cité pour d'autres raisons                      .....                      &amp; : membre de la même famille, document correspondant</p>		

2