PCT ORGANISATION MONDIALE DE LA PROPRIETE INTELLECTUELLE
Bureau international

DEMANDE INTERNATIONALE PUBLIEE EN VERTU DU TRAITE DE COOPERATION EN MATIERE DE BREVETS (PCT)

(51) Classification internationale des brevets 3: H04N 7/16	A1	(11) Numéro de publication internatinoale: WO 80/01636
		(43) Date de publication internationale: 7 août 1980 (07.08.80)

(21) Numéro de la demande internationale: PCT/FR80/00019

(22) Date de dépôt international: 5 février 1980 (05.02.80)

(31) Numéro de la demande prioritaire: 79/02994

(32) Date de priorité: 6 février 1979 (06.02.79)

(33) Pays de priorité: FR

(71) Déposants: TELEDIFFUSION DE FRANCE [FR/FR]; 21/27, rue Barbès, 92120 Montrouge (FR). L'ETAT FRANCAIS, représenté par LE SECRETAIRE D'ETAT AUX POSTES ET TELECOMMUNICATIONS (CENTRE NATIONAL D'ETUDES DES TELECOMMUNICATIONS) [FR/FR]; 38/40, rue du Général Leclerc, 92131 Issy les Moulineaux (FR).

(72) Inventeur: GUILLOU, Louis, Claude; 7, rue de l'Ise, 35230 Bourgbarre (FR).

(74) Mandataire: SOCIETE FRANCAISE POUR LA GESTION DES BREVETS D'APPLICATION NUCLEAIRE BREVATOME; 25, rue de Ponthieu, 75008 Paris (FR).

(81) Etats désignés: BR, JP, SU.

Publiée
Avec rapport de recherche internationale

(54) Title: VIDEOTEX SYSTEM PROVIDED WITH INFORMATION ACCESS CONTROL MEANS

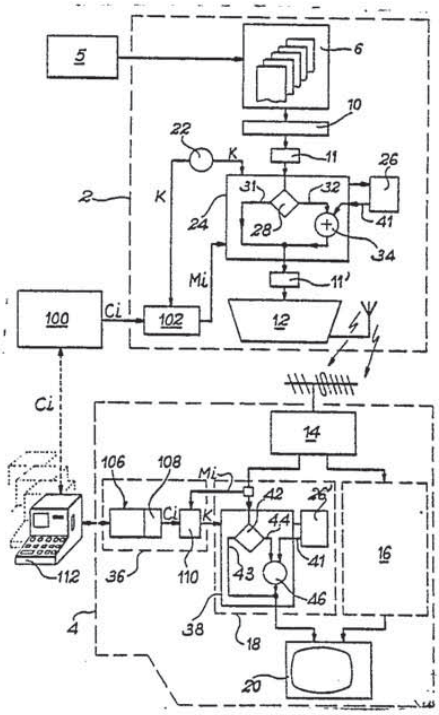
(54) Titre: SYSTEME DE VIDEOTEX MUNI DE MOYENS DE CONTROLE D'ACCES A L'INFORMATION

(57) Abstract

The system comprises a transmission center (2) and receivers (4). The transmission center comprises a magazine composition source (6), a locking automaton (24), a service key generator (22), a transmission circuit (12). A subscriber center (100) provides subscription keys which are transformed into messages by a circuit (102). The group of messages composes a special page for control of access. In the receiver the service key is returned by a circuit (36) by means of the messages received and by means of a subscription key inscribed into a support (106) and the unlocking of the information is effected in a circuit (38). The subscription supports are loaded in a set (112). Application to the ANTIOPE and TITAN systems.

(57) Abrégé

Le système de l'invention comprend un centre d'émission (2) et des postes récepteurs (4). Le centre d'émission comprend une source de composition d'un magazine (6), un automate de verrouillage (24), un générateur de clé de service (22), un circuit d'émission (12). Un centre d'abonnements (100) fournit des clés d'abonnement qu'un circuit (102) transforme en messages. L'ensemble des messages compose une page spéciale de contrôle d'accès. Dans le poste récepteur la clé de service est restituée par un circuit (36) à l'aide des messages reçus et d'une clé d'abonnement inscrite dans un support (106) et le déverrouillage des informations est effectué dans un circuit (38). Les supports d'abonnement se chargent dans un poste (112). Application aux systèmes ANTIOPE et TITAN.



UNIQUEMENT A TITRE D'INFORMATION

Codes utilisés pour identifier les Etats parties au PCT, sur les pages de couverture des brochures publiant des demandes internationales en vertu du PCT.

AT	Autriche	**LI**	Liechtenstein
AU	Australie	**LU**	Luxembourg
BR	Brésil	**MC**	Monaco
CF	République Centrafricaine	**MG**	Madagascar
CG	Congo	**MW**	Malawi
CH	Suisse	**NL**	Pays-Bas
CM	Cameroun	**NO**	Norvège
DE	Allemagne, République fédérale d'	**RO**	Roumanie
DK	Danemark	**SE**	Suède
FR	France	**SN**	Sénégal
GA	Gabon	**SU**	Union soviétique
GB	Royaume-Uni	**TD**	Tchad
HU	Hongrie	**TG**	Togo
JP	Japon	**US**	Etats-Unis d'Amérique
KP	République populaire démocratique de Corée		

SYSTEME DE VIDEOTEX MUNI DE MOYENS DE CONTROLE D'ACCES A L'INFORMATION.

La présente invention a pour objet un système de vidéotex muni de moyens de contrôle d'accès à l'information.

Elle trouve une application dans la transmission et l'affichage d'informations sur des récepteurs de télévision à des fins quelconques de distraction, d'information, ou d'enseignement. L'invention s'applique essentiellement au système dit "ANTIOPE" (Acquisition Numérique et Télévisualisation d'Images Organisées en Pages d'Ecriture), et au système dit "TITAN" (Terminal Interactif de Télétexte à Appel par Numérotation). On sait qu'il s'agit essentiellement, pour le premier, d'un système de vidéotex diffusé (donc unidirectionnel) permettant d'insérer sur des voies de télévision des informations alphanumériques organisées en pages et en magazines. Pour le second, il s'agit d'un système de vidéotex interactif (donc bidirectionnel) compatible avec le système ANTIOPE et permettant l'accès à des bases de données (informations générales, annuaires, etc...) et à des services interactifs (transactions, messages, enseignement) par le réseau téléphonique.

Dans le système ANTIOPE, la diffusion des informations s'effectue par une procédure dite "DIDON" (Diffusion de Données Numériques) qui est une procédure de diffusion par paquets, compatible avec la diffusion du signal de télévision.

De nombreux articles ou demandes de brevets ont déjà décrit ces systèmes. On se réfèrera par la suite essentiellement au système ANTIOPE dont on pourra trouver une description détaillée, notamment dans les documents suivants :

- l'article de Y. GUINET intitulé "Etude comparative des systèmes de télétexte en radiodiffusion. Quelques avantages de la diffusion des données par paquets appliquée au télétexte" paru dans la revue de l'U.E.R. cahier Technique, n° 165, Octobre 1977, pages 242 à 253 ;
- l'article de B. MARTI et M. MAUDUIT intitulé "ANTIOPE, service de Télétexte" paru dans la revue "Radiodiffusion Télévision", 9ème année, n° 40, novembre-décembre 1975, 5/5 pages 18 à 23 ;
- la "Spécification du système de télétexte ANTIOPE", éditée par le Centre Commun d'Etudes de Télévision et Télécommunications (CCETT) ;
- la demande de brevet français n° 75 18319, déposée le 6 juin 1975 et intitulée "Système de diffusion de données" ;
- la demande de brevet français n° 76 27212, déposée le 6 septembre 1976 et intitulée "Système de transmission numérique et d'affichage de texte sur un écran de télévision" ;
- la demande de brevet français n° 76 29034, déposée le 22 septembre 1976 et intitulée "Perfectionnements aux systèmes de transmission numérique et d'affichage de textes sur un écran de télévision" ;
- la demande de certificat d'addition français n° 77 17625, déposée le 3 juin 1977 et intitulée "Système de diffusion de données".

Le système ANTIOPE étant ainsi largement connu, il ne sera pas décrit ici en détail. On se bornera à en rappeler les principes essentiels, dans le but de faciliter la compréhension de l'invention. Pour tout détail de conception ou de réalisation, on pourra toujours se reporter aux documents cités plus haut, qui eux-mêmes renvoient à d'autres, tous ces documents devant être considérés comme incorporés à la présente description.

La figure 1 rappelle très schématiquement les éléments essentiels d'un système de télétexte ANTIOPE. Un tel système comprend un centre d'émission 2 et des postes récepteurs 4, 4', etc...

Le centre d'émission reçoit des informations d'une ou de plusieurs sources 5 et il comprend :

- un moyen 6 de composition d'un magazine constitué de pages organisées en rangées de caractères, si cette composition n'a pas déjà été effectuée par le dépositaire de l'information ;
- un circuit 10 de mémorisation du magazine sous forme de signaux numériques groupés en octets (8 éléments binaires) ;
- une jonction 11 reliée au circuit 10 ;
- un multiplexeur 12 de diffusion servant à la constitution de paquets d'octets et à l'insertion des informations dans les lignes d'un signal de télévision, ce moyen mettant en oeuvre la procédure DIDON évoquée plus haut.

Chaque poste récepteur comprend :

- un circuit 14 de réception et de démodulation dudit signal de télévision ;
- une voie 16 de traitement des signaux vidéo d'image ;
- une voie 18 de traitement des signaux numériques, cette voie comprenant notamment un décodeur de données numériques, et enfin,
- un organe 20 de visualisation.

Dans un tel système, le flux d'informations depuis les dépositaires d'informations jusqu'aux centres de diffusion présente les caractéristiques générales suivantes.

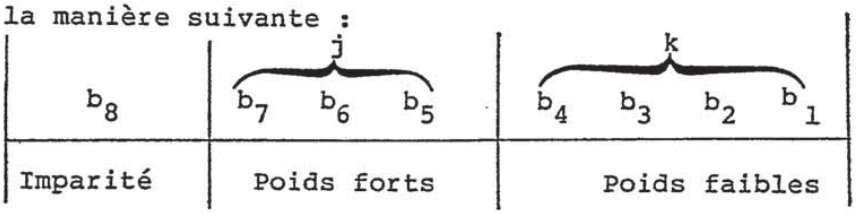
La source 5, qui est une banque de données dépositaires d'informations est, par exemple, un service météorologique, la Bourse, une agence d'infor-

mations, etc... Cette banque alimente le moyen de composition 6 qui met ces informations en page au format ANTIOPE.

Pour fixer les ordres de grandeur, on peut indiquer que, dans le cas d'un magazine expérimental réalisé pour les valeurs boursières, on peut trouver environ 80 pages contenant en moyenne 800 octets, soit au total 64000 octets. Un tel magazine boursier utilise une ressource de 10 lignes par trame. Une ligne de télévision dure 64µs et peut véhiculer 32 octets utiles, et il y a 50 trames par seconde. Ainsi, la ressource de une ligne/trame permet de transmettre 50 X 32 X 8 = 12800 b/s (éléments binaires par seconde). L'ensemble d'un tel magazine est donc transmis en $\frac{64 \times 8}{12{,}8 \times 10}$ = 4 secondes, ce qui signifie que le magazine est transmis cycliquement avec une période de 4 secondes.

On observera qu'une ligne interactive reliant le centre de diffusion au dépositaire de l'information fonctionne typiquement à 4800 b/s et que c'est cette différence de vitesse par rapport à la diffusion à 12800 b/s qui explique la nécessité d'une mémorisation de l'information au niveau de la source de diffusion.

Dans le système ANTIOPE, les octets véhiculant l'information sont notés traditionnellement de la manière suivante :



où l'élément binaire b_8 est un élément d'imparité, autrement dit un élément tel que le nombre total de "1" figurant dans l'octet soit impair.

Selon cette notation, l'octet (j/k) = (4/7) correspond ainsi à l'octet 11000111.

Les octets se divisent en octets de commande et en octets de données. Les octets de commande indiquent notamment des en-têtes et des fins de pages ainsi que des en-têtes et des fins de rangées. Les octets de données, insérés entre des octets de commande, correspondent à des caractères contenus dans les rangées. Tous ces octets, qu'ils soient de commande ou de données, comprennent un élément binaire de poids fort qui est un élément d'imparité.

L'ensemble des codes, identifiés par de tels octets, s'organise selon un tableau qui est le suivant :

				b_7	0	0	0	0	1	1	1	1
				b_6	0	0	1	1	0	0	1	1
				b_5	0	1	0	1	0	1	0	1
b_4	b_3	b_2	b_1	k \ j	0	1	2	3	4	5	6	7
0	0	0	0	0								
0	0	0	1	1								
0	0	1	0	2								
0	0	1	1	3								
0	1	0	0	4								
1	1	1	1	15								

Dans ce tableau :

- les colonnes 0 et 1 qui correspondent aux octets dont les 6^e et 7^e éléments binaires sont nuls ($b_6 = b_7 = 0$), contiennent des octets de commande ;
- les colonnes 2 et 3 contiennent essentiellement des nombres et des signes de ponctuation ;
- les colonnes 4 et 5 contiennent principalement des majuscules,
- les colonnes 6 et 7 contiennent principalement des minuscules.

A titre d'exemple, une page courante d'information, accessible à l'usager se présente sous la forme suivante :

1) - Elle contient tout d'abord un en-tête de page, qui se compose des codes de commande (ETX) FF RS NP_1 NP_2 NP_3 :
où : ETX est un code qui termine la page précédente,
FF est un code qui indique une nouvelle page,
RS est un drapeau de page,
NP_1, NP_2, NP_3 sont des codes indiquant un numéro de page allant de 001 à 999.

2) - Après l'en-tête de page, figure une rangée "zéro" : US OO C_1 C_2 C_3.....RC LF,
où : US est un drapeau de rangée,
OO indique le rang zéro,
C_1, C_2, C_3 sont des codes complémentaires,
RC LF terminent la rangée.
La rangée zéro peut contenir aussi un nom de service, une date, une heure et éventuellement des indications de taxation. Cette rangée zéro ne véhicule pas d'information constituant le service. Elle fait partie de la procédure.

3) - Après la rangée zéro, viennent des rangées d'information comprenant d'abord un en-tête de rangée qui se compose des codes (RC LF) US NR_1 NR_2,
où : RC LF terminent la rangée précédente,
US est un drapeau de rangée,
NR_1, NR_2 constituent le numéro de rangée qui va de 01 à 24.
viennent ensuite des octets de données d_1, d_2...d_n. Ces octets sont insérés entre l'en-tête de rangée courante et soit une fin de

la rangée - début d'une autre rangée - soit une fin de page. Ces octets d_1, d_2,...d_n représentent l'information constituant le service diffusé. L'élément d'information dans un tel système est donc la rangée visualisable.

Il existe également d'autres pages que ces pages courantes d'information. Elles sont accessibles fonctionnellement par l'intermédiaire des codes complémentaires C_1, C_2, C_3 contenus dans la rangée zéro. Ce sont par exemple des pages de garde et d'alarme. Toutes ces pages font partie de la procédure. Il existe enfin une page de sommaire que l'on peut considérer comme faisant partie des données.

Ces rappels à propos du système ANTIOPE étant effectués, on peut aborder maintenant le problème que se propose de résoudre la présente invention.

L'avènement des services de type ANTIOPE ou TITAN soulève la question de leur taxation, c'est-à-dire de la mise en oeuvre d'un système permettant l'identification et le contrôle des audiences. Cette question se pose d'ailleurs plus généralement pour tout service diffusé tendant à rentabiliser les réseaux de diffusion par une meilleure utilisation des ressources.

Une taxation de type à abonnement constitue une relation à la fois souple et durable entre un service et ses usagers. C'est en diffusion surtout qu'un tel mode de taxation trouve sa justification.

Une taxation de type à la consommation peut également être retenue ; ce mode de taxation est fondamental pour les systèmes "interactifs" (dans lesquels un dialogue s'instaure entre l'abonné et la source d'information, comme c'est le cas pour TITAN) ; mais il reste secondaire dans les systèmes à diffusion (dans lesquels les informations sont transmises de manière unidirectionnelle vers des abonnés, comme c'est le cas pour ANTIOPE).

Des systèmes intermédiaires, dits "quasi-interactifs" peuvent se présenter, dans lesquels on modifie sans cesse le contenu de la source de diffusion pour satisfaire aux requêtes des usagers qui sont transmises par un réseau public de données. L'avènement des nouveaux moyens de diffusion à très grande capacité (satellites) développera beaucoup ce mode quasi-interactif, rendant alors nécessaire la mise en oeuvre d'un système de contrôle de l'accès à l'information offerte.

Ce problème du contrôle d'accès pose avant tout celui du verrouillage de l'information à l'émission et du déverrouillage à la réception. Ce problème doit naturellement être résolu en tenant compte de la spécificité du système de télétexte à contrôler. En particulier, la méthode de brouillage des informations et celle de recouvrement de l'intelligibilité des informations, ne doit pas pénaliser les performances du système.

Or, on sait que les messages traduits dans le langage ANTIOPE sont caractérisés par une importante redondance, de manière que soit minimisée l'incidence des erreurs de transmission sur l'intelligibilité de l'information diffusée. C'est ainsi que les textes alphabétiques sont intrinsèquement très redondants ; de même que la plupart des dessins en semi-graphique ; que les commandes de visualisation de caractères utilisent des caractères d'échappement ; que les numérotations de pages et de lignes mettent en oeuvre des codes de Hamming ; que tous les octets constituant un magazine sont transmis avec imparité, etc... Aucun effort n'est donc fait pour comprimer l'information et la méthode de recouvrement de l'intelligibilité de l'information doit donc respecter cette redondance et ne pas propager les conséquences néfastes des erreurs de transmission, difficilement contrôlables en diffusion.

Les moyens de recouvrement de l'intelligibilité d'une information préalablement verrouillée constituent en quelque sorte une "serrure électronique", et seule la mise en oeuvre d'une clé appropriée permet de recouvrer l'intelligibilité de l'information verrouillée.

La première question qui se pose alors, est celle de la place à attribuer à cette serrure électronique dans le système à contrôler. En effet, dans le cas du système de télétexte, deux procédures sont mises en jeu : la procédure de transport (DIDON) et la procédure de service (ANTIOPE). A quel niveau de procédure doit-on disposer cette serrure ?

L'invention répond à cette question en proposant une serrure qui est attachée au niveau du service. Cette façon de procéder présente plusieurs avantages. Elle respecte tout d'abord les contraintes de synchronisation et de non propagation des erreurs de transmission. De plus, elle est indépendante du réseau de transport utilisé par le vidéotex. Enfin, elle ne demande aucun réaménagement des normes ANTIOPE existantes et s'accommodera d'une éventuelle évolution de ces normes.

En d'autres termes, et selon une première caractéristique de l'invention, le verrouillage de l'information constituant un magazine ANTIOPE est effectué au niveau de la source de diffusion. De façon plus précise, les moyens de verrouillage se situent en amont du multiplexeur DIDON qui, sur le schéma de la figure 1, porte la référence 12.

Une place ayant été assignée au verrouillage, reste la question de l'objet auquel s'applique ce verrouillage.

L'invention répond à cette seconde question en proposant un moyen dont la fonction est de verrouiller exclusivement l'information véhiculée dans les

rangées visualisables des pages ordinaires du magazine. En d'autres termes, le verrouillage n'affecte pas les codes de commande figurant dans les colonnes 0 et 1 du tableau des codes indiqué plus haut et notamment, les codes ETX, FF, RS, RC, LF et US. Il n'affecte que les codes de données d_1, d_2, etc... C'est là la seconde caractéristique de l'invention.

Enfin, l'invention se propose de résoudre un troisième problème qui est celui du respect de l'imparité des octets diffusés.

Tous ces buts sont atteints par l'utilisation, selon l'invention, d'un automate de verrouillage qui comprend un moyen pour former une suite d'octets chiffrants dont les éléments binaires, notés c_1 à c_8 sont engendrés de la manière suivante :

- c_1, c_2, c_3, c_4 et c_5 sont prélevés à la sortie d'un générateur de suite pseudo-aléatoire, réinitialisé au début de chaque rangée visualisable par une clé de service K et par les numéros de la page et de la rangée considérée ;
- c_6 et c_7 sont à zéro, et
- c_8 est un élément de parité.

Ainsi, la suite chiffrante obtenue est composée d'octets pairs. Ces octets sont notés C_1, $C_2 \ldots C_n$ ou, de façon générique C_j. Les octets clairs constituant une rangée d'information forment une suite notée d_1, $d_2 \ldots d_n$ ou de façon générique d_j. Ces octets sont impairs et ils sont verrouillés par les octets chiffrants selon les règles suivantes :

A chaque nouvel octet clair de la rangée visualisable, on prélève un octet de la suite chiffrante.Deux cas peuvent se présenter :

- Si l'octet clair appartient aux colonnes 0 et 1 du tableau des codes ($b_6 = b_7 = 0$) l'octet clair est transmis tel quel, et l'octet chiffrant n'est pas utilisé ;

- Si l'octet clair n'appartient pas aux colonnes 0 ou 1, alors l'octet clair et l'octet chiffrant sont combinés par un circuit logique "OU-exclusif" pour constituer un octet diffusé : $D_j = d_j \oplus C_j$, où le signe $\oplus$ représente l'opération logique "OU-exclusif".

Du fait de la parité des octets chiffrants, les octets diffusés sont impairs, tout comme les octets clairs, ce qui répond bien à l'exigence posée plus haut.

En outre, l'opération "OU-exclusif" se traduit par une substitution à l'octet clair d'un octet diffusé appartenant au même groupe de colonnes que l'octet clair, à savoir :

- le groupe des colonnes 2 et 3 qui contient essentiellement les nombres et des signes de ponctuation,
- le groupe des colonnes 4 et 5 qui contient principalement des majuscules,
- et le groupe des colonnes 6 et 7 qui contient principalement des minuscules.

Enfin, les octets appartenant aux colonnes 0 et 1 ne sont pas modifiés, en particulier les octets correspondant aux codes ETX, FF, RS, RC, LF et US qui sont transmis tels quels. De plus, du fait de la nullité des 6^e et 7^e éléments binaires des octets chiffrants, il n'y a pas introduction de nouveaux octets appartenant à ces colonnes. La transparence souhaitée est donc assurée.

Ainsi, tous les buts énoncés plus haut sont-ils atteints par ce moyen de verrouillage mis en oeuvre selon l'invention.

Pour renforcer le caractère d'inviolabilité de la serrure ainsi constituée, la clé de service K est avantageusement modifiée de manière aléatoire à des intervalles déterminés et relativement courts (par exemple de l'ordre de quelques minutes).

Il reste alors, à la réception, à déverrouiller l'information. Pour ce faire, le récepteur doit comprendre un générateur d'octets déchiffrants qui délivre des octets formés comme suit :

- les 5 éléments binaires de faible poids sont prélevés dans une suite quasi-aléatoire obtenue par un générateur réinitialisé à chaque en-tête de rangée par la clé de service K, par le numéro de page et par le numéro de rangée considérés ;
- les 6^e et 7^e éléments binaires sont nuls, et
- le 8^e élément binaire est forcé à zéro.

Les règles de déverrouillage sont analogues aux règles de verrouillage : à chaque nouvel octet reçu appartenant à une rangée verrouillée, un nouvel octet déchiffrant est engendré. Deux cas peuvent se présenter :

- Si l'octet reçu appartient aux colonnes 0 et 1, il est transmis tel quel aux circuits d'interprétation ;
- Si l'octet reçu n'appartient pas aux colonnes 0 et 1, (parce que ses 6^e et/ou 7^e éléments binaires ne sont pas nuls) il est combiné par un circuit OU-exculsif à l'octet déchiffrant avant la poursuite de l'interprétation.

L'interprétation du langage est donc intimement entrelacée avec le déverrouillage des rangées d'information, et la robustesse de la structure du langage ANTIOPE diffusé n'est pas affectée par les opérations de verrouillage.

Ces généralités sur l'invention ayant été exposées, la définition précise de l'objet de l'invention semble alors pouvoir être formulée de la manière suivante :

"Système de vidéotex comprenant un centre d'émission d'information et des postes récepteurs, le centre d'émission comprenant :

- un moyen de composition d'un magazine constitué de pages organisées en rangées de caractères, si ce moyen n'est pas déjà contenu dans la source d'information,
- un circuit de mémorisation du magazine sous forme de signaux numériques groupés en octets (8 éléments binaires), ces octets comprenant des octets de commande et des octets de données, les octets de commande indiquant notamment des en-têtes de fins de pages ainsi que des en-têtes et des fins de rangées, les octets de données correspondant à des caractères contenus dans chaque rangée, tous ces octets de commande et de données comprenant un élément binaire de poids fort qui est un élément d'imparité, les octets ayant des 6^e et 7^e éléments binaires nuls étant des octets de commande,
- une jonction reliée au circuit de mémorisation,
- un multiplexeur de diffusion servant à l'insertion des informations dans les lignes d'un signal de télévision,

ce centre d'émission comprenant en outre des moyens de chiffrement de l'information utilisant une clé de service, chaque poste récepteur comprenant :

- un circuit de réception et de démodulation dudit signal de télévision,
- une voie de traitement des signaux vidéo d'image,
- une voie de traitement des signaux numériques contenant notamment un décodeur de signaux numériques, et
- un organe de visualisation,

chaque poste récepteur comprenant en outre des moyens de déchiffrement de l'information chiffrée utilisant ladite clé de service, le système étant caractérisé en ce que :

A) - les moyens de chiffrement du centre d'émission comprennent :

a) un générateur délivrant un signal numérique représentant une clé de service K, cette clé changeant de manière aléatoire à des intervalles déterminés,

b) un automate de verrouillage comprenant :

i) un comparateur à une entrée reliée au circuit de mémorisation du magazine d'où il reçoit des octets clairs, ce comparateur étant apte à distinguer parmi ces octets clairs, ceux dont les 7^e et 6^e éléments binaires sont nuls, ce comparateur ayant deux sorties, la première véhiculant ces octets à 7^e et 6^e éléments binaires nuls et qui est reliée au multiplexeur de diffusion à travers la jonction, et la seconde véhiculant les octets clairs d_j dont les 7^e et/ou 6^e éléments binaires ne sont pas nuls,

ii) un circuit logique OU-exclusif à deux entrées, dont l'une reliée à la deuxième sortie du comparateur d'où elle reçoit les octets clairs d_j à 6^e et/ou 7^e éléments binaires non nuls, ce circuit logique ayant une sortie qui véhicule des octets chiffrés impairs D_j, les octets chiffrés étant dirigés ensuite vers le multiplexeur de diffusion à travers la jonction ;

c) un générateur d'octets chiffrants commandé par l'automate de verrouillage d'où il reçoit des octets indiquant les numéros de page et les numéros de rangées des données à transmettre ainsi que le signal correspondant

à la clé de service, ce générateur d'octets délivrant, pour chaque octet de données d_j d'une rangée visualisable un octet chiffrant C_j, cet octet possédant un 8^e élément binaire de parité et des 7^e et 6^e éléments binaires nuls, cet octet étant appliqué à l'autre entrée du circuit logique.

B) - les moyens de déchiffrement de chaque poste récepteur comprennent :

d) un générateur d'un signal numérique représentant la clé de service K en cours dans le centre d'émission,

e) un automate de déverrouillage comprenant :

i) un comparateur à une entrée reliée au décodeur de signaux numériques du poste récepteur d'où il reçoit les octets chiffrés, ce comparateur étant apte à distinguer, parmi ces octets chiffrés, ceux dont les 7^e et 6^e éléments binaires sont nuls, ce comparateur ayant deux sorties, la première véhiculant ces octets dont les 7^e et 6^e éléments binaires sont nuls, cette première sortie étant reliée directement à l'organe de visualisation, la seconde véhiculant les octets chiffrés D_j dont les 7^e et/ou 6^e éléments binaires ne sont pas nuls,

ii) un circuit logique OU-exclusif à deux entrées, l'une reliée à la deuxième sortie du comparateur d'où elle reçoit les octets chiffrés D_j, ce circuit logique ayant une sortie qui véhicule des octets déchiffrés d_j dirigés ensuite vers l'organe de visualisation ;

f) un générateur d'octets déchiffrants commandé par l'automate de déverrouillage qui lui transmet les octets indiquant les numéros de page et les numéros de rangées des données transmises et le signal correspondant à la clé de service en cours K, ce générateur d'octets déchiffrants possédant une sortie qui délivre, pour chaque octet chiffré reçu, un octet déchiffrant C_j possédant un élément binaire de poids fort qui est forcé à zéro et des 7^e et 6^e éléments binaires nuls.

De tels moyens de verrouillage et de déverrouillage permettent de résoudre de manière avantageuse le problème de la taxation évoqué plus haut. A cette fin, l'invention propose d'utiliser, en plus de la clé de service, dont le rôle vient d'être défini, des clés d'abonnement qui sont engendrées de manière aléatoire par un centre de gestion des taxations. Ces clés ont une durée de vie relativement longue (de 1 à 12 mois), par rapport à celle de la clé de service (qui est de l'ordre de quelques minutes).

Pour illustrer le fonctionnement de ce système à double clé, on peut prendre un exemple de schéma d'abonnement qui utiliserait quatre types d'abonnements : 1 mois, 3 mois, 6 mois et un an. En plus de sa durée, un abonnement est caractérisé par son mois de début. Avec un tel schéma, durant un mois donné et pour un service donné, il y a donc 22 clés d'abonnement susceptibles d'être utilisées par les usagers : une clé mensuelle, trois clés trimestrielles, six clés semestrielles et douze clés annuelles.

Chaque mois, le centre de gestion des taxations fournit à chaque centre de diffusion une liste de 22 clés d'abonnement en cours pour chaque service

diffusé par ce centre. En outre, il fournit à des points de vente d'abonnements, une autre liste de 4 clés qui vont débuter le mois suivant (un mois, trois mois, six mois et un an), pour chaque service, avec les tarifs des abonnements.

Une machine appropriée, installée dans chaque point de vente, inscrit certaines de ces clés sous forme de blocs d'abonnements sur des supports prévus à cet effet (par exemple des cartes intelligentes de type "carte de crédit"). Ces cartes sont ensuite introduites par les usagers du service dans leur poste récepteur.

Pour chaque service payant, toutes les cinq minutes environ, une nouvelle clé du service K est engendrée au hasard, par chaque centre de diffusion intéressé. Ainsi, au cours d'une session d'un service (une heure ou quelques heures), quelques dizaines de clés de service peuvent se succéder.

Dès qu'un centre de diffusion engendre une nouvelle clé de service K, il calcule, pour chaque clé d'abonnement en cours C_i pour ce service, un message M_i par un algorithme $M_i = F_{C_i}(K)$, les clés C_i jouant le rôle de paramètres.

Ainsi, pour un service doté du schéma d'abonnement indiqué plus haut, à tout instant, 22 messages différents sont en vigueur. La durée de vie d'un message est égale à celle de la clé du service K, et pour un service donné, à tout instant, il existe autant de messages qu'il y a de clés d'abonnement en cours.

L'ensemble des messages M_i en vigueur constitue l'information de contrôle d'accès associée au service diffusé. Cette information de contrôle d'accès n'est évidemment pas verrouillée par la serrure électronique.

Ce système particulier de taxations sur abonnement faisant intervenir deux clés, l'une d'abonnement, l'autre de service, fait l'objet, dans ses éléments essentiels, de la demande de brevet français n° EN 79 02995 déposée le 6 février 1979 et intitulée "Système de transmission d'information entre un centre d'émission et des postes récepteurs, ce système étant muni d'un moyen de contrôle de l'accès à l'information transmise".

Une application particulière de ce système est prévue dans le cadre de la présente invention, aux systèmes de vidéotex (ANTIOPE ou TITAN). En l'occurrence, les messages M_i sont groupés dans une page spéciale, dite page de contrôle d'accès, qui est remise à jour à chaque changement de clé du service. La page de contrôle d'accès est diffusée cycliquement, comme les pages ordinaires d'information constituant le service. Elle n'est cependant pas verrouillée par la serrure électronique. La page de contrôle d'accès est lue systématiquement par le récepteur à la mise en relation avec le service, puis à chaque mise à jour de cette page, au cours de la consultation du service, mais elle n'est pas visualisable.

Les messages sont donc, en fait, des motifs de synchronisation primaire de la serrure et ces motifs sont interprétables par un algorithme fournissant la clé du service. Cet algorithme est de la forme : $K = G_{C_i}(M_i)$, et il est développé par un circuit de restitution (qui peut d'ailleurs faire partie du support d'abonnement, lequel contient déjà la clé d'abonnement C_i) à qui les messages M_i sont fournis. Ce circuit fournit donc à l'automate de déverrouillage la clé du service K, qui lui permet de déverrouiller l'information reçue.

Quant au support d'abonnement, qui contient, d'une part, les clés d'abonnement C_i et qui peut, d'autre part, contenir le circuit de restitution de la clé de service K, il fait l'objet, en soi, d'une autre demande de brevet français n° EN 79 02996 déposée le 6 février 1979 et intitulée "Carte d'abonnement pour récepteur de vidéotex et poste de chargement de ladite carte".

De toute façon, les caractéristiques et avantages de la présente invention apparaîtront mieux après la description qui suit, d'exemples de réalisation donnés à titre explicatif et nullement limitatif. Cette description se réfère à des dessins annexés sur lesquels :

- la figure 1, déjà décrite, représente le schéma synoptique d'un système de télétexte ANTIOPE, conforme à l'art antérieur ;
- la figure 2 représente le schéma synoptique d'un système selon l'invention ;
- la figure 3 représente le schéma d'un circuit permettant de matérialiser un polynome générateur primitif particulier ;
- la figure 4 représente un générateur de suite pseudo-aléatoire constitué par une combinaison de trois circuits du type de la figure précédente ;
- la figure 5 représente le schéma synoptique d'un générateur d'octets chiffrants ou d'octets déchiffrants ;
- la figure 6 représente un diagramme illustrant les différents états que peut prendre un automate de verrouillage ;
- la figure 7 illustre le schéma synoptique d'un système de télétexte muni des moyens de contrôle d'accès fonctionnant à l'aide de clés d'abonnement ;

- la figure 8 représente les moyens mis en oeuvre dans le centre de diffusion pour verrouiller l'information ;

- la figure 9 représente le schéma synoptique d'un récepteur selon l'art antérieur ;

- la figure 10 représente le schéma synoptique des moyens à insérer dans le récepteur du type de la figure précédente pour effectuer le déverrouillage de l'information.

Le système de vidéotex de l'invention est représenté, sous la forme qu'il prend dans le cas du système ANTIOPE, par le schéma de la figure 2. Ce système comprend des éléments connus déjà représentés sur la figure 1, à savoir :

- dans le centre d'émission 2 :
  - un moyen 6 d'élaboration d'un magazine constitué de pages organisées en rangées de caractères, si ce moyen n'est pas déjà dans la source d'information,
  - un circuit 10 de mémorisation du magazine sous forme de signaux numériques,
  - une pluralité de jonctions 11 reliées au circuit 10, et
  - un multiplexeur 12 de diffusion servant à l'insertion des informations dans les lignes d'un signal de télévision,
- dans chaque poste récepteur 4 :
  - un circuit 14 de réception et de démodulation dudit signal de télévision,
  - une voie 16 de traitement des signaux vidéo d'image,
  - une voie 18 de traitement des signaux numériques contenant notamment un décodeur de signaux numériques, et
  - un organe de visualisation 20.

Selon l'invention, le système comprend en outre :

A) - dans le centre d'émission 2 :

a) un générateur 22 délivrant un signal numérique représentant une clé de service K, cette clé changeant de manière aléatoire à des intervalles déterminés qui sont par exemple, de l'ordre de quelques minutes ;

b) un automate de verrouillage 24 comprenant :

i) un comparateur 28 à une entrée reliée au circuit 10 de mémorisation du magazine d'où il reçoit des octets clairs ; ce comparateur est apte à distinguer, parmi ces octets clairs, ceux dont les 7^e et 6^e éléments binaires sont nuls ; ce comparateur possède deux sorties 31 et 32, la première véhiculant ces octets à 7^e et 6^e éléments binaires nuls et qui est reliée au multiplexeur 12 de diffusion (à travers une jonction 11'), et la seconde véhiculant les octets clairs d_j dont les 7^e et/ou 6^e éléments binaires ne sont pas nuls ;

ii) un circuit logique 34 de type OU-exclusif à deux entrées, l'une reliée à la deuxième sortie 32 du comparateur 28 d'où elle reçoit les octets clairs d_j à 6^e et 7^e éléments binaires non nuls ; ce circuit logique possède une sortie qui véhicule des octets chiffrés impairs D_j, les octets chiffrés étant dirigés ensuite (à travers la jonction 11') vers le multiplexeur de diffusion 12 ;

c) un générateur 26 d'octets chiffrants C_j, commandé par l'automate 24 d'où il reçoit des octets indiquant les numéros de page et les numéros de rangées des données à transmettre et le signal correspondant à la clé de service K ; ce générateur d'octets 26 délivre, pour chaque octet de données d_j d'une rangée visualisable, un octet chifffrant C_j, cet octet possédant un 8^e élément binaire de parité et des 7^e et 6^e éléments binaires nuls, cet octet étant appliqué à la seconde entrée de la porte 34.

B) - dans chaque poste récepteur 4 :

d) un circuit 36 délivrant un signal numérique représentant la clé de service K en cours dans le poste d'émission,

e) un automate de déverrouillage 38 comprenant :

i) un comparateur 42 à une entrée recevant les octets chiffrés ; ce comparateur est apte à distinguer, parmi ces octets chiffrés, ceux dont les 7^e et 6^e éléments binaires sont nuls, ce comparateur ayant deux sorties 43 et 44, la première véhiculant ces octets dont les 7^e et 6^e éléments binaires sont nuls, cette première sortie étant reliée à l'organe de visualisation 20, la seconde véhiculant les octets chiffrés D_j dont les 7^e et/ou 6^e éléments binaires ne sont pas nuls,

ii) un circuit logique 46 de type OU-exclusif à deux entrées, l'une reliée à la sortie 44 du comparateur d'où elle reçoit les octets chiffrés D_j, ce circuit logique ayant une sortie qui véhicule des octets déchiffrés d_j, qui ensuite sont dirigés vers l'organe de visualisation 20.

f) un générateur 26' d'octets déchiffrants, commandé par l'automate de déverrouillage, d'où il reçoit les octets indiquant les numéros de page, les numéros de rangées des données transmises, et, le signal correspondant à la clé de service en cours K ; ce générateur d'octets déchiffrants possède une sortie 41 qui délivre, pour chaque octet chiffré reçu, un octet déchiffrant C_j possédant un élément binaire de poids fort qui est forcé à zéro et des 7^e et 6^e éléments binaires nuls, ces octets étant appliqués à la seconde entrée de la porte 46.

On va décrire en détail les différents éléments de cet ensemble en commençant par les générateurs d'octets chiffrants 26, et déchiffrants 26' qui sont d'ailleurs quasi-identiques.

Le générateur d'octets chiffrants (ou déchiffrants) fait appel à un générateur de suite pseudo-aléatoire, lequel peut être de différents types. On peut utiliser, par exemple, un circuit de chiffrement par bloc monté en mode quasi-synchrone. A cette fin, on peut mettre en oeuvre l'algorithme dit "D.E.S." (Data Encryption Standard) décrit dans US Department of Commerce, NBS, FIPS, PUB 46, 15 janvier 1977.

Mais, on peut aussi engendrer une telle suite pseudo-aléatoire grâce à des polynomes générateurs combinés par une logique non linéaire et c'est ce cas particulier qu'on va décrire maintenant à l'aide des figures 3 et 4.

On rappellera tout d'abord quelques notions concernant ce type de polynomes et on indiquera ensuite un moyen de les obtenir.

La littérature spécialisée fournit des tables de polynomes irréductibles sur le corps de Galois de 2. Ces polynomes sont représentés de manière

condensée par une suite de chiffres, par exemple "642 015". La numérotation est faite en octal, de manière à ce que chaque chiffre représente trois éléments binaires, chaque élément représentant un coefficient du polynome. Dans l'exemple du polynome 642 015, les correspondances octal-binaire-coefficients du polynome sont les suivantes :

6			4			2			0			1			5		
1	1	0	1	0	0	0	1	0	0	0	0	0	0	1	1	0	1

$x^{17} + x^{16} + x^{14} + x^{10} + x^{3} + x^{2} + 1$

Il s'agit donc d'un polynome de degré 17 qui possède 7 termes.

En partant d'un ensemble de valeurs initiales de 17 éléments binaires non tous nuls (a_0, a_1, $a_2 \ldots a_{16}$), on définit la suite engendrée par le polynome 642 015, par la relation :

$a_i = a_{i-1} + a_{i-3} + a_{i-7} + a_{i-14} + a_{i-15} + a_{i-17}$ modulo 2 pour $i \geq 1$.

La suite ainsi obtenue est périodique et de longueur maximale $2^{17}-1$, et on dit alors que le polynome générateur est primitif. Si α désigne une racine de ce polynome, on peut montrer que l'ensemble $0, 1, \alpha, \alpha^2, \alpha^3 \ldots, \alpha^{(2^{17}-1)}$ possède une structure de corps : c'est le corps muni des lois d'addition par OU-exclusif et de multiplication modulo le polynome de Galois d'extension $CG(2^{17})$.

Pour illustrer la manière de mettre en oeuvre de tels polynomes, on reprendra l'exemple du polynome 642 015. Il peut être réalisé à l'aide de 17 bascules de type D et 6 portes "OU-exclusif", connectées comme il est indiqué sur la figure 3, où les bascules portent la référence 50 et les portes la référence 52.

L'interface avec l'extérieur comprend 4 connexions : une entrée 54, une sortie 56, une connexion d'horloge 58 et une remise à zéro 60. Il faut y ajouter une connexion d'alimentation et une connexion de masse non représentées.

L'intervalle de temps minimum t_{min} entre deux coups d'horloge est lié au retard apporté à la propagation du signal dans les portes et les bascules. Dans le circuit de la figure 3, on a $t_{min} = 3$ retards porte + 1 retard bascule.

A titre indicatif, avec des circuits de type SN 74273 pris pour constituer les huit bascules D, le retard obtenu est de 23 ns, et avec des circuits SN 7486 pris pour constituer les quatre portes OU-exclusif, le retard obtenu est de 40 ns. La fréquence maximum d'horloge est alors de 7 MHz environ.

Le circuit de la figure 3 fonctionne de la manière suivante. Un ordre "remise à zéro" est d'abord émis pour imposer un état connu ; puis, le circuit est initialisé en présentant n éléments binaires sur la connexion d'entrée 54 en synchronisme avec n tops d'horloge sur la connexion d'horloge 58. Le générateur est ensuite prêt à fonctionner. Il délivre un élément binaire chaque fois qu'il reçoit un nouveau top d'horloge.

Pour augmenter la complexité de la suite obtenue et renforcer de ce fait le générateur, on peut combiner plusieurs polynomes de la manière suivante :

Soit trois polynomes primitifs, T, R et S. Il s'agit par exemple des polynomes :
T : 642 015 (degré t = 17),
R : 3 020 365 (degré r = 19),
S : 21 042 104 211 (degré s = 31).

On peut combiner ces polynomes par une relation logique non linéaire, par exemple $(R.\overline{S}) \oplus (S.T)$ où le point correspond à l'opération ET, la barre à l'opération NON et le signe $\oplus$ à l'opération OU-exclusif.

La période de la suite obtenue est égale au plus petit commun multiple entre (2^t-1), (2^r-1) et (2^s-1) ; dans l'exemple envisagé où les trois nombres $(2^{17}-1)$, $(2^{19}-1)$ et $(2^{31}-1)$ sont premiers, la période est environ $1{,}4.10^{17}$.

La complexité de la suite obtenue est égale à $r(s+1) + st$, soit $19.32 + 31.17 = 1135$.

Ainsi, alors qu'un polynome primitif de degré r a pour complexité r, ce qui signifie que tout état de l'automate permettant de l'obtenir est une combinaison linéaire des r racines du polynome générateur, donc un élément du corps d'extension $CG(2^r)$, la complexité de l'ensemble $R.\overline{S} \oplus ST$ est $r(s+1) + st$, c'est-à-dire que tout état de l'automate ainsi constitué est un élément du corps d'extension $CG(2^{r(s+1)+st})$ et que l'automate linéaire équivalent et minimum possède $r(s+1) + st$ bascule D.

A propos de ces propriétés des combinaisons de polynomes, on pourra se reporter à l'article de Edwin L. KEY intitulé "Structure and Complexity of non-linear binary Sequence Generators" publié dans la revue I.EEE IT 22, N° 6, novembre 1976, pages 732 à 736.

La combinaison de polynomes en question s'obtient à l'aide du circuit 61 de la figure 4. Sur cette figure, le circuit 62 engendre le polynome T, le circuit 64 le polynome R et le circuit 66 le polynome S. Les portes 68 et 70 sont des portes ET, la seconde étant reliée au circuit 66 par une porte inverseuse 72 ; la porte 74 est une porte OU-exclusif. L'ensemble du circuit possède une entrée 76, une sortie 78, une connexion d'horloge 80 et une connexion de remise à zéro 82.

Ce moyen particulier apte à engendrer une suite pseudo-aléatoire ayant été décrit, on va aborder maintenant la description du générateur d'octets chiffrants (ou déchiffrants) qui utilise ce moyen.

La structure d'un tel générateur est représentée schématiquement sur la figure 5. Elle comprend essentiellement un générateur de suite pseudo-aléatoire 61 tel que celui qui vient d'être décrit à propos de la figure 4, un ensemble de huit bascules 84 de type D, reliées à un bus 86, et un séquenceur 88 relié également au bus 86 et au générateur 61 et qui gère les tops d'horloge et les entrées-sorties du circuit. L'interface avec l'extérieur est composé de 16 connexions respectivement :

- de sélection 91, de lecture 92, d'écriture 93 et de remise à zéro 94, pour ce qui est du contrôle,
- d'horloge 95, de chiffrage/déchiffrage 96, d'alimentation 97 et de masse 98 pour ce qui est de la mise en oeuvre, et
- huit connexions de données B_1 à B_8 pour les entrées-sorties.

Avant de préciser le fonctionnement de ce circuit, il faut rappeler la différence qu'il y a entre les octets chiffrants utilisés dans le centre d'émission et les octets déchiffrants utilisés dans les postes récepteurs.

A l'émission, les octets chiffrants sont des octets pairs appartenant aux colonnes 0 et 1 du tableau donné plus haut ($c_6 = c_7 = 0$). Ainsi, la parité des octets chiffrés est la même que celle des octets clairs et l'on sait que ces octets sont impairs.

A la réception, l'élément binaire d'imparité des octets reçus est vérifié puis remplacé par un élément binaire de validation. Aussi, les octets dé-

chiffrants comportent-ils un élément binaire de poids fort qui est forcé à zéro ($c_8 = 0$), ce qui les distinguent des octets chiffrants qui possèdent un 8^e élément binaire de parité.

Dans ces conditions, le fonctionnement du circuit de la figure 5 est le suivant. Ce circuit peut recevoir trois ordres :

- "remise à zéro",
- "lire", et
- "écrire".

a) - L'ordre "remise à zéro" se traduit par la remise à zéro des 75 bascules que comprend le circuit (8 bascules 84, 17 bascules dans le générateur 62, 9 dans le générateur 64 et 31 dans le générateur 66). Cet ordre permet de remettre l'automate dans un état connu ;

b) - L'ordre "lire" se traduit par la prise en compte des données sur le bus 86 afin d'initialiser les huit bascules 84 de l'interface. Ces données sont transmises aux trois générateurs 62, 64 et 66 par huit tops d'horloge, ce qui produit huit éléments binaires nouveaux. Ces huit éléments binaires nouveaux sont utilisés comme suit :

- les cinq premiers positionnent les cinq premières bascules 84 de l'interface,
- les trois derniers sont "oubliés",
- Les 6ème et 7ème bascules sont forcées à zéro,
- la 8ème bascule impose la parité correcte si l'on est en position "chiffrement", et elle est forcée à zéro si l'on est en position "déchiffrement" pour les raisons qui viennent d'être rappelées ;

c) - L'ordre "écrire" se traduit par l'affichage, sur le bus, des états des huit bascules 84. Ces huit bascules sont ensuite remises à zéro

et huit tops d'horloge permettent de créer huit nouveaux éléments binaires utilisés comme pour l'ordre "lire".

L'initialisation du générateur d'octets s'effectue à l'aide de la clé de service (qui est constituée de 64 éléments binaires, soit 8 octets notés k_1 à k_8) du numéro de rangée (qui varie de 1 à 24 et qui est codé sur deux octets notés NR_1 et NR_2) et du numéro de page (qui varie de 001 à 999 et qui est codé sur trois octets notés NP_1, NP_2 et NP_3).

Cette initialisation du générateur d'octets est pratiquée au début de chaque rangée d'information, à l'aide de 8 octets particuliers, obtenus à partir des huit octets qui définissent la clé du service et des cinq octets définissant le numéro de page et le numéro de rangée.

Ces huit octets sont, par exemple :
$k_1 \oplus NR_1$, $k_2 \oplus NR_2$, $k_3 \oplus NP_1$, $k_4 \oplus NP_2$, $k_5 \oplus NP_3$, $k_6 \oplus NP_3$, $k_7 \oplus NR_1$, $k_8 \oplus NR_2$.

Ainsi, au début de chaque rangée d'information, le générateur d'octets subit les opérations suivantes :

- remise à zéro,
- lire ($k_1 \oplus NR_1$),
- lire ($k_2 \oplus NR_2$),
- lire ($k_3 \oplus NP_1$),
- lire ($k_4 \oplus NP_2$),
- lire ($k_5 \oplus NP_3$),
- lire ($k_6 \oplus NP_3$),
- lire ($k_7 \oplus NR_1$),
- lire ($k_8 \oplus NR_2$).

Ensuite, pour chaque octet de la rangée, l'ordre est donné au générateur d'écrire un nouvel octet. Il est essentiel d'engendrer systématiquement un octet chiffrant pour chaque octet d'information, afin de maintenir la synchronisation, malgré les erreurs de transmission.

En désignant par d_1, d_2, d_3... les octets clairs d'une rangée, par C_1, C_2, C_3 les octets chiffrants délivrés par le générateur et par D_1, D_2, D_3... les octets chiffrés, on a le tableau suivant de la suite des codes :

Octets clairs : US NR_1 NR_2 d_1 d_2 d_3 d_4 d_5 d_6 d_7...

Octets chiffrants : C_1 C_2 C_3 C_4 C_5 C_6 C_7...

Octets chiffrés : US NR_1 NR_2 D_1 D_2 D_3 D_4 D_5 D_6 D_7...

avec $D_i = \begin{cases} \overline{d_i}, \text{ si } d_i \text{ appartient aux colonnes 0 ou 1,} \\ d_i \oplus C_i \text{ si } d_i \text{ appartient aux colonnes 2 à 7.} \end{cases}$

Le tableau de la suite des codes rencontrée au déchiffrement serait analogue avec permutation des lignes octets clairs et octets chiffrés.

Le générateur d'octets chiffrants ou déchiffrants ayant été décrit, on va aborder maintenant le principe de l'automate de verrouillage qui met en oeuvre ce générateur. La structure de cet automate est illustrée sur la figure 2 déjà décrite. Son fonctionnement est le suivant.

L'automate de verrouillage reçoit, du circuit 10, une suite d'octets qui modifient à chaque fois sa situation. Cette situation est définie par trois paramètres, qui dépendent respectivement du numéro de page reçu (lequel varie entre 001 et 999), du numéro de rangée (lequel va de 00 à 24) et de son "état", lequel peut prendre six formes différentes :

- Etat 0 : l'automate attend un début de page ;
- Etat 1 : l'automate laisse passer le numéro de la page (NP_1 NP_2 NP_3) en l'enregistrant ;
- Etat 2 : l'automate attend un début de rangée ;
- Etat 3 : l'automate laisse passer le numéro de la rangée (NR_1 NR_2) en l'enregistrant ;
- Etat 4 : l'automate chiffre la rangée d'information après avoir réinitialisé le générateur d'octet ;

- Etat 5 : l'automate laisse passer la rangée zéro (le rôle de cette rangée zéro sera analysé plus loin).

La figure 6 illustre l'évolution de l'automate en fonction de la nature des octets qu'il reçoit. Les notations FF, RS, US ont déjà été définies. Les différents états de l'automate sont représentés par des chiffres cerclés correspondant à la liste précédente (les états 1 et 3 sont en traits mixtes pour les distinguer des autres car il s'agit d'états passifs). Au début du fichier, l'automate est dans l'état 0 (à gauche du diagramme). Si l'octet reçu est différent de RS, l'automate reste dans cet état 0. D'où la flèche qui part du 0 cerclé et qui y revient. Lorsque l'octet reçu est un octet RS (correspondant à un drapeau de page), l'automate passe dans l'état 1 et laisse passer le numéro de rangée en l'enregistrant ; puis il passe à l'état 2 où il attend un début de rangée, etc...

Finalement, le seul état où l'automate effectue un chiffrement est l'état 4 où il traite une range d'informations d'une page accessible par numérotation.

En entrant dans l'état 4, l'automate de verrouillage réinitialise le générateur d'octets chiffrants par 9 ordres successifs : un ordre "remise à zéro", suivi par 8 ordres "lire", comme il vient d'être décrit. Ensuite, l'automate de verrouillage engendre un nouvel octet chiffrant C pour chaque nouvel octet clair d. Si l'octet clair d n'a pas ses 6e et 7e éléments binaires à zéro, l'automate reste dans l'état 4 et verrouille cet octet par $d \oplus C$ puis va saisir un nouvel octet. Si l'octet clair d est un octet de commande ($b_6 = b_7 = 0$), quatre cas se présentent :

- l'octet clair est un "US" (drapeau de rangée) ; l'automate passe à l'état 3 ;
- l'octet clair est un "FF" (fin de page) ; l'automate passe à l'état 0 ;

- l'octet clair est un "RS" (drapeau de page) ; l'automate passe à l'état 1 ;
- l'octet clair n'est ni "US" ni "FF", ni "RS", l'automate reste à l'état 4.

De toute façon, dans ces cas là, l'octet clair est transmis tel quel, et l'automate va saisir un nouvel octet.

Après avoir décrit les moyens de verrouillage et de déverrouillage qui sont le premier objet de la présente invention, on va décrire les moyens de contrôle d'accès à l'information, qui constituent, en combinaison avec les premiers moyens, le second objet de l'invention.

La figure 7 illustre le schéma synoptique du système de l'invention muni de ces moyens de contrôle d'accès. Tel que représenté, ce système comprend, en plus des éléments qui ont déjà été décrits à propos de la figure 2 :

A) - un centre de gestion d'abonnements 100 qui engendre des signaux numériques correspondant aux clés d'abonnement C_i, ces clés changeant de manière aléatoire à intervalles longs de l'ordre du mois et selon des schémas analogues à celui qui a été indiqué plus haut à titre d'exemple ;

B) - dans le centre d'émission :

- un circuit 102 de formation de messages M_i qui reçoit du circuit 100 les signaux correspondant auxdites clés d'abonnement C_i et du générateur 22 le signal correspondant à la clé de service K. Ces messages sont obtenus à l'aide d'un algorithme $F_{C_i}(K)$ paramétré par les C_i, qui sera explicité plus loin. Le circuit 102 délivre autant de messages M_i qu'il y a de clés d'abonnement C_i, ces messages changeant avec la clé de service K. L'ensemble de ces messages est organisé en une page spéciale 104 dite page de contrôle d'accès. Cette page est transmise cycliquement par le multiplexeur 12, mais n'est

pas visualisable ; sa structure sera indiquée plus loin ;

C) - dans chaque poste récepteur :

i) un support d'abonnement 106 qui contient une mémoire 108 dans laquelle est inscrit au moins un bloc d'abonnement représentant l'une des clés d'abonnement C_i ;

j) un circuit 110 de restitution de la clé de service K, relié, d'une part, au décodeur de signaux numériques du circuit 14 d'où il reçoit l'ensemble des messages M_i constituant la page de contrôle d'accès, et d'autre part, à la mémoire 108 du support d'abonnement d'où il reçoit la clé d'abonnement C_i. Ce circuit 110 développe un algorithme $K = G_{C_i}(M_i)$ qui permet de restituer le signal correspondant à la clé de service K employée dans le poste d'émission ; cet algorithme sera explicité plus loin ;

D) - au moins un poste de chargement 112 relié au centre de gestion d'abonnement 100 d'où il reçoit les signaux correspondant aux différentes clés d'abonnement C_i engendrées par ce centre ; chacun de ces postes est apte à recevoir temporairement des supports d'abonnement et à inscrire dans leur mémoire 108 l'une des clés d'abonnement C_i.

On va décrire maintenant la manière de composer la page de contrôle d'accès, à partir de clés d'abonnement C_i et de la clé de service K. Pour cela, on décrira tout d'abord la structure des signaux numériques représentant les clés d'abonnement, puis on exposera l'algorithme de calcul des messages et on donnera enfin la constitution de la page de contrôle d'accès.

Les clés d'abonnement sont engendrées au centre de gestion des abonnements 100 qui fournit des listes aux centres d'émission 2 et aux postes 112 de chargement des cartes.

De façon plus précise, le centre de gestion des abonnements fournit :

- au centre d'émission :
  les clés d'abonnement en cours pour les services qui le concernent ainsi que les consignes d'exploitation sur la durée de vie à donner à K la clé de service ;
- aux postes de chargement des cartes :
  les blocs d'abonnement à vendre pour les services qui les concernent ainsi que les tarifs à appliquer.

Un bloc d'abonnement est composé par exemple de quatre champs :

1) un "code de service" de 16 éléments binaires qui désigne le service considéré,
2) un "indice d'abonnement" de 8 éléments binaires qui caractérise un abonnement pour un service considéré. Deux de ces éléments binaires indiquent le type d'abonnement (1, 3, 6 ou 12 mois) et les six autres indiquent le mois de début d'abonnement (1 à 60 modulo 5 ans),
3) une "clé d'abonnement" de 128 éléments binaires qui est l'information fondamentale du bloc,
4) un "code de redondance cyclique" de 16 éléments binaires.
   Ce code porte sur les 152 éléments binaires précédents et permet de vérifier le bloc d'abonnement avant d'en faire usage.

Un bloc d'abonnement est donc composé de 168 éléments binaires, soit 21 octets. Un tel bloc peut aisément être inscrit dans un support genre "carte de crédit" qui serait muni d'une mémoire PROM (Programmable Read Only Memory) d'une capacité de 4096 éléments binaires utilisables à cette fin. Une telle carte pourrait accueillir jusqu'à 24 blocs d'abonnement ayant les caractéristiques indiquées.

Le calcul des messages à partir des clés d'abonnement C_i et de la clé K est effectué dans le centre d'émission par le circuit 102 qui est organisé autour d'un microprocesseur. Ce circuit est programmé pour mettre en oeuvre un algorithme qui s'appuie sur deux corps de Galois ayant pour caractéristiques les nombres premiers de Mersenne $2^{61}-1$ et $2^{127}-1$. Cet algorithme utilise les clés d'abonnement C_i (127 éléments binaires) et la clé du service K (56 éléments binaires), de la manière suivante :

1°) On forme un mot π de redondance de confusion qui comprend 61 éléments binaires engendrés au hasard à chaque mise en oeuvre de l'algorithme ;

2°) on calcule π^{-1}, inverse de π modulo $2^{61}-1$ par un programme arithmétique utilisant une variante de l'algorithme d'Euclide ;

3°) on effectue une première multiplication par un autre programme arithmétique : $\nu = K.\pi^{-1}$ modulo $(2^{61}-1)$;

4°) on calcule γ, inverse de C modulo $2^{127}-1$, par un programme similaire à celui de 2°) ;

5°) enfin, on calcule le message par un programme similaire à 3°) : $M = \gamma.(\nu + 2^{64}.\pi)$ modulo $(2^{127}-1)$.

Les programmes nécessaires à ces calculs peuvent être développés par un microprocesseur du type 8080, de la Société INTEL.

La structure de la page de contrôle d'accès qui rassemble de tels messages est la suivante :

... (ETX) FF RS NP_1 NP_2 NP_3
US 0 0 C_1 C_2 C_3 C_4 <bloc d'en-tête>
RC LF US NR_1 NR_2 <bloc d'accès>
RC LF US NR'_1 NR'_2 <bloc d'accès>

RC LF US NR^i_1 NR^i_2 <bloc d'accès> ETX (FF).

Les codes qui ouvrent la page ont déjà été définis. La rangée zéro (US 00) commence par trois codes complémentaires C_1, C_2 et C_3 traditionnellement

destinés à permettre l'insertion de pages fonctionnelles dans les magazines.

Pour indiquer que cette page particulière est une page de service à ne pas visualiser, le quatrième élément binaire de C_2 est à 1. Un quatrième octet de code complémentaire C_4 est utilisé avec $b_1 = b_2 = b_3 = b_4 = 1$ pour identifier la page de contrôle d'accès.

Cette page est modifiée chaque fois que l'on change K, la clé de service. Pour signaler cet évènement, on fait usage du 4e élément binaire de C_1, traditionnellement utilisé pour indiquer une nouvelle mise à jour, et qui est porté à 1 pendant une période suivant immédiatement cette mise à jour.

La rangée zéro se poursuit par un bloc d'entête qui comprend le code du service (16 éléments binaires), le mois en cours (6 éléments binaires) et un code de redondance cyclique de 16 éléments binaires.

Viennent ensuite les différentes rangées de la page de contrôle d'accès. Ces rangées débutent par un numéro de rangée suivi d'un bloc d'accès, et il y a autant de blocs d'accès (donc de rangées) qu'il y a de blocs d'abonnement. La numérotation de ces rangées peut avantageusement être la suivante.

Comme il a été exposé plus haut, pour un service donné, un bloc d'abonnement est caractérisé par un indice d'abonnement qui se compose d'un code à 8 éléments binaires. De même, il a été indiqué qu'à un moment donné, il pouvait y avoir 22 blocs d'abonnement en cours, si l'on retient le schéma d'abonnement indiqué plus haut pour 24 rangées disponibles.

Or, un numéro de rangée s'étend sur 2 octets possédant chacun 4 éléments binaires utiles (les quatre autres constituent un code de Hamming) soit au total également 8 éléments binaires. Il en résulte qu'il est possible de prendre l'indice d'abonnement comme numéro de rangée dans la page de contrôle d'accès.

Par conséquent, dans une variante avantageuse, le numéro d'une rangée de la page de contrôle d'accès donne l'indice de l'abonnement auquel se rapporte le bloc d'accès qui suit.

Quant auxdits blocs d'accès, ils se composent de deux champs :

1) un message de 127 éléments binaires utiles plus 1 élément binaire à zéro,
2) un code de redondance cyclique de 16 éléments binaires.

Un bloc d'accès comprend donc 144 éléments binaires utiles qui s'étendent sur 24 octets à raison de 6 éléments binaires utiles, complétés par $b_7 = 1$ et b_8 en imparité.

Ayant décrit l'organisation générale du système de l'invention, on va décrire maintenant plus en détail les moyens particuliers qu'il faut insérer dans le centre de l'émission et dans les postes récepteurs, pour pouvoir effectivement contrôler l'accès à l'information, selon le processus qui vient d'être décrit. On s'intéressera tout d'abord aux moyens disposés dans le centre d'émission pour aborder ensuite ceux des postes récepteurs.

Dans le centre d'émission, ces moyens s'insèrent entre la source de diffusion (circuit 10 sur la figure 2) et le circuit émetteur (multiplexeur DIDON 12 sur cette même figure 2), deux jonctions 11 et 11' les encadrant. Ces moyens sont illustrés en détail sur la figure 8. Le circuit représenté sur cette figure comprend deux ensembles :

1) un ensemble lent 120 (constitué en pratique par un microprocesseur convenablement programmé et interfacé) qui comprend un circuit 122 qui assure le contrôle et la gestion des horloges (durée de vie de la clé de serrure K, décision d'insertion des pages

de contrôle d'accès) et un circuit 124, pour la composition de la page de contrôle d'accès, ce circuit recevant les messages M_i du circuit 102 déjà mentionné. Les circuits 122 et 102 sont reliés à un générateur aléatoire 134. L'opérateur fournit à cet ensemble 120 les consignes horaires d'exploitation par une connexion 126 et les blocs d'abonnement en cours au début de chaque session du service considéré, par une connexion 128. Cet ensemble lent est interfacé par deux mémoires : la mémoire 130 qui contient K, la clé de service, et la mémoire 132 qui contient la page de contrôle d'accès. Des connexions de contrôle non représentées permettent de véhiculer les ordres : verrouillage-arrêt, insertion de la page de contrôle d'accès, lecture de K, acquittement sur fin de page de magazine, acquittement sur fin de page de contrôle d'accès et bien sûr, remise à zéro.

2) un ensemble rapide 134 (constitué par une logique câblée permettant des débits de l'ordre de 20 k octets/seconde) qui comprend l'automate de verrouillage 24 déjà décrit et le générateur d'octets chiffrants 26, dont la structure et le fonctionnement ont été exposés plus haut à propos de la figure 5.

L'intérêt du montage décrit est que l'exploitant est maître de la vie de la clé de service K, et des instants d'insertion de la page de contrôle d'accès dans le magazine verrouillé.

Avant d'en venir aux moyens à insérer dans chaque poste récepteur pour permettre l'accès à l'information, il est nécessaire de préciser la structure de ce récepteur telle qu'on la trouve dans le système ANTIOPE classique, structure qui n'avait été qu'ébauchée sur les figures 1 et 2.

Cette structure est représentée sur la figure 9 qui correspond à la figure 2 de la demande de brevet

français déjà mentionnée n° EN 76/27212 déposée le 6 Septembre 1976.

Le récepteur illustré sur la figure 9 comporte les grands blocs fonctionnels déjà mentionnés sur les figures 1 et 2, à savoir : un circuit de réception et de démodulation 14, une voie 16 de traitement des signaux image, une voie 18 de traitement des signaux numériques et un moyen de visualisation 20. Le circuit 14 délivre d'une part, le son à un haut-parleur 15, et d'autre part, le signal vidéo à un décodeur de couleur et générateur de balayage 19. Les signaux de couleur B_1, V_1 et R_1, ainsi que la luminance L_1 issus du circuit 19 sont transmis au tube 140 à travers un commutateur vidéo 141.

Le poste récepteur illustré, comporte dans la voie 18 de traitement des signaux numériques, un séparateur vidéo-données 142 (qui fonctionne selon la procédure DIDON pour extraire une suite d'octets du signal analogique) dont l'entrée est reliée à la sortie vidéo du circuit 14. Ce séparateur a sa sortie reliée à un circuit de première sélection 143 (qui fonctionne lui aussi selon la procédure DIDON, de manière à extraire les octets véhiculés dans une voie numérique) semblable à l'équipement terminal décrit dans la demande de brevet n° EN 75/18319 déjà citée. La sortie du circuit 143 est reliée par une jonction 144 du type décrit dans la demande de brevet français n° EN 74/13136 déposée le 16 Avril 1974, à un circuit sélecteur de page et décodeur de données 145 dont la sortie est reliée à l'entrée d'une mémoire de pages 146. Un clavier d'abonné 147 est relié aux entrées de commande des blocs 143 et 145 et au commutateur 141. La sortie de la mémoire 146 est reliée à l'entrée d'un générateur de caractères 148. Les sorties de signaux du générateur 148 sont reliées aux entrées de couleur R_2, V_2 et B_2 du commutateur vidéo 141, ainsi qu'à une entrée de luminance L_2.

Le fonctionnement de ce circuit étant déjà décrit dans la demande n° EN 76/27212 déjà citée, il ne sera pas réexposé ici. On rappellera simplement qu'à la sortie du circuit DIDON analogique 142, les données sont des octets structurés en paquets enveloppés par une procédure de huit octets d'en-tête, dont trois octets de numéro de voie. Le circuit DIDON numérique 143 sélectionne une voie numérique, c'est-à-dire laisse passer les données utiles des paquets sélectionnés, d'après leur numéro de voie.

La jonction 144 ne joue pas un rôle essentiel dans le système de l'invention, mais est surtout utile pour faciliter la séparation physique au niveau transport (DIDON) et au niveau service (ANTIOPE).

La sélection de page et le décodage des pages sélectionnées sont effectués dans le circuit 145. Cet ensemble décode une page d'information, rangée par rangée, et vient remplir la mémoire de page 146. Cette mémoire peut présenter une capacité de 1001 mots de 16 éléments binaires (25 rangées de 40 caractères plus un mot de contrôle), chaque caractère étant codé sur 16 éléments binaires en forme et attributs de visualisation.

Ce rappel étant effectué, on peut aborder la question des modifications à apporter à ce récepteur pour pouvoir effectuer le contrôle d'accès.

La serrure électronique conforme à l'invention étant rattachée au niveau du service, comme il a été souligné plus haut, elle n'a aucune incidence sur la procédure DIDON. Le fonctionnement des circuits 142 (DIDON analogique) et 143 (DIDON numérique) n'est donc en rien modifié. Au travers de la jonction 144, passent donc toujours des données structurées en pages, elles-mêmes structurées en rangées. Parmi ces pages, on distingue toujours des pages fonctionnelles, accessibles grâce aux codes complémentaires, et des pages d'information, accessibles par numérotation sur le clavier 147.

Cependant, parmi ces pages fonctionnelles, une nouvelle variété a été introduite à l'émission en vue du contrôle : c'est la page de contrôle d'accès, dont la structure a été décrite plus haut. En outre, selon l'invention, les pages d'informations ont été verrouillées rangée par rangée, hormis la rangée zéro considérée comme partie intégrante de la procédure. Le circuit 145 doit donc être complété pour pouvoir prendre en compte ces deux éléments nouveaux.

Les compléments nécessaires sont de deux types :

1) Au niveau du décodage des pages d'information : le décodeur doit effectuer le déverrouillage rangée par rangée en utilisant un générateur d'octets semblable à celui qui est mis en oeuvre à l'émission ;

2) Au niveau du traitement des pages fonctionnelles : le décodeur doit connaître le mode d'emploi des pages de contrôle d'accès et il doit également savoir dialoguer avec une carte d'abonnement pour obtenir K, la clé de service.

Ces compléments comprennent à la fois du logiciel venant compléter les logiciels déjà existants dans le circuit 145, ainsi que du matériel spécialisé. Ce dernier est représenté sur la figure 10. Il s'agit du générateur d'octets déchiffrants 26' (qui est analogue au générateur 26 de la figure 5), de la carte d'abonnement 106, du circuit 110 permettant de restituer la clé K à partir de M_i et C_i, du comparateur 42 permettant de distinguer les octets appartenant aux colonnes 0 et 1 qui sont interprétés directement pour configurer la mémoire 146, les octets des colonnes 2 à 7 qui passent par la porte OU-exclusif 46, avant d'être interprétés et dirigés vers la mémoire 146.

Au niveau du logiciel, le décodage des pages d'informations par le circuit 145, ne pose pas de problème particulier, car dans sa conception classique (décrite dans la demande de brevet déjà citée), ce circuit a déjà conscience des numéros de page et de rangée.

Il a même conscience de la rangée zéro puisqu'il y analyse les codes complémentaires. Le numéro de page lui sert à sélectionner la page, tandis que le numéro de rangée lui sert à positionner un pointeur dans la mémoire de page 146.

Dans la présente invention, en présence d'une nouvelle rangée d'informations, le décodeur 145 initialise le générateur d'octets déchiffrants 26', selon le processus indiqué plus haut à propos de la figure 5 et qui fait appel à neuf ordres successifs.

Ensuite, pour chaque octet de la rangée, le décodeur 145 provoque la génération d'un octet déchiffrant C_j ($c_6 = c_7 = c_8 = 0$), et si l'octet reçu D_j n'est pas un code de commande (colonnes 0 et 1) ce que vérifie le comparateur 42, le décodeur le combine par "OU-exclusif" avec l'octet déchiffrant dans la porte 46.

Au niveau du traitement des pages fonctionnelles, le circuit 145 possède les programmes permettant l'analyse et l'usage des pages de contrôle d'accès. Le circuit localise dans la mémoire 108 de la carte 106, à l'adresse appropriée, un bloc d'abonnement valide d'où il extrait l'indice de l'abonnement. Puis il recherche dans la page d'accès, la rangée correspondant à cet indice d'abonnement (puisque, comme on l'a vu, les rangées sont numérotées par les indices). Il y récupère le bloc d'accès et en extrait le message M_i. Ce message est transmis au circuit 110 qui calcule alors la clé K à l'aide de la clé d'abonnement C_i figurant dans le bloc d'abonnement qui vient d'être localisé dans la carte.

Pour restituer cette clé K à partir de M_i et C_i, le circuit 110 (qui peut faire partie intégrante de la carte et constituer le support 36) est programmé pour développer un algorithme $K = G_{C_i}(M_i)$ qui est,

comme à l'émission, un algorithme à double corps.
Les opérations sont les suivantes :

1) Le message M_i (127 éléments binaires utiles) est saisi octet par octet et une multiplication par C_i est effectuée sur le premier corps CG $(2^{127}-1)$. On forme ainsi un mot μ :

$$\mu = M \cdot C \quad \text{modulo } (2^{127}-1)$$

D'après la construction de M à l'émission, les éléments binaires 1 à 61 de μ représentent le mot ν, tandis que les éléments binaires 65 à 125 représentent le mot π. Bien entendu, les éléments binaires 62, 63, 64, 126 et 127 doivent être nuls. S'ils ne le sont pas, on met le mot ν à zéro avant de continuer le calcul.

2) π et ν sont multipliés sur le deuxième corps CG$(2^{61}-1)$, ce qui fait disparaître la redondance de confusion et l'on obtient $K = \nu.\pi$ modulo $(2^{61}-1)$.
Un nouveau test de vraisemblance intervient ici puisque K ayant 56 éléments binaires utiles, les éléments 57, 58, 59, 60 et 61 doivent être nuls. Dans le cas contraire K est mis à zéro avant la poursuite des opérations.

3) Les 56 éléments binaires utiles de K sont alors disponibles sous forme de huit octets impairs.

La description qui précède se rapport à un système ANTIOPE dans lequel l'information est transmise par la procédure DIDON dans les lignes d'un signal de télévision. Mais, il va de soi que l'invention est plus générale, car elle ne présuppose pas un procédé particulier de transport de l'information puisque, comme il a été souligné plus haut, le verrouillage s'effectue au niveau du service et non au niveau du transport.

Il va de soi également que le système ANTIOPE n'a été pris que comme exemple de réalisation et que l'invention pourraît être appliquée à d'autres sytèmes sans difficulté pour l'homme de l'art, et notamment au système TITAN ou encore aux systèmes CEEFAX ou ORACLE, ou VIEWDATA ou PRESTEL.

REVENDICATIONS

1. Système de vidéotex comprenant un centre d'émission d'information et des postes récepteurs, le centre d'émission comprenant :

- un moyen (6) de composition d'un magazine constitué de pages organisées en rangées de caractères, si ce moyen n'est pas déjà contenu dans la source d'information,
- un circuit (10) de mémorisation du magazine sous forme de signaux numériques groupés en octets (8 éléments binaires), ces octets comprenant des octets de commande et des octets de données, les octets de commande indiquant notamment des en-têtes de fins de pages ainsi que des en-têtes et des fins de rangées, les octets de données correspondant à des caractères contenus dans chaque rangée, tous ces octets de commande et de données comprenant un élément binaire de poids fort qui est un élément d'imparité, les octets ayant des 6e et 7e éléments binaires nuls étant des octets de commande,
- une jonction (11) reliée au circuit (10), et
- un multiplexeur (12) de diffusion servant à l'insertion des informations dans les lignes d'un signal de télévision,

ce centre d'émission comprenant en outre des moyens de chiffrement de l'information utilisant une clé de service,

chaque poste récepteur comprenant :

- un circuit (14) de réception et de démodulation dudit signal de télévision,
- une voie (16) de traitement des signaux vidéo d'image,
- une voie (18) de traitement des signaux numériques contenant notamment un décodeur de signaux numériques, et
- un organe de visualisation (20),

chaque poste récepteur comprenant en outre des moyens de déchiffrement de l'information chiffrée utilisant ladite clé de service,

le système étant caractérisé en ce que :

A) les moyens de chiffrement du centre d'émission comprennent :

a) un générateur (22) délivrant un signal numérique représentant une clé de service (K), cette clé changeant de manière aléatoire à des intervalles déterminés,

b) un automate de verrouillage (24) comprenant :

i) un comparateur à une entrée reliée au circuit de mémorisation du magazine d'où il reçoit des octets clairs, ce comparateur étant apte à distinguer parmi ces octets clairs, ceux dont les 7e et 6e éléments binaires sont nuls, ce comparateur ayant deux sorties, la première véhiculant ces octets à 7e et 6e éléments binaires nuls et qui est reliée au multiplexeur de diffusion à travers la jonction, et la seconde véhiculant les octets clairs d_j dont les 7e et/ou 6e éléments binaires ne sont pas nuls,

ii) un circuit logique OU-exclusif à deux entrées, dont l'une reliée à la deuxième sortie du comparateur d'où elle reçoit les octets clairs d_j à 6e et/ou 7e éléments binaires non nuls, ce circuit logique ayant une sortie qui véhicule des octets chiffrés impairs D_j, les octets chiffrés étant dirigés ensuite vers le multiplexeur de diffusion à travers la jonction ;

c) un générateur d'octets chiffrants commandé par l'automate de verrouillage d'où il reçoit des octets indiquant les numéros de pages et les numéros de rangées des données à transmettre ainsi que le signal correspondant à la clé de service, ce générateur d'octets délivrant, pour chaque octet de données d_j d'une rangée visualisable un octet chiffrant C_j, cet octet possédant

un 8e élément binaire de parité et des 7e et 6e éléments binaires nuls, cet octet étant appliqué à l'autre entrée du circuit logique,

B) les moyens de déchiffrement de chaque poste récepteur comprennent:

d) un générateur d'un signal numérique représentant la clé de service (K) en cours dans le centre d'émission,

e) un automate de déverrouillage comprenant :

i) un comparateur à une entrée reliée au décodeur de signaux numériques du poste récepteur d'où il reçoit les octets chiffrés, ce comparateur étant apte à distinguer, parmi ces octets chiffrés, ceux dont les 7e et 6e éléments binaires sont nuls, ce comparateur ayant deux sorties, la première véhiculant ces octets dont les 7e et 6e éléments binaires sont nuls, cette première sortie étant reliée directement à l'organe de visualisation, la seconde véhiculant les octets chiffrés D_j dont les 7e et/ou 6e éléments binaires ne sont pas nuls,

ii) un circuit logique OU-exclusif à deux entrées, l'une reliée à la deuxième sortie du comparateur d'où elle reçoit les octets chiffrés D_j, ce circuit logique ayant une sortie qui véhicule des octets déchiffrés d_j dirigés ensuite vers l'organe de visualisation ;

f) un générateur d'octets déchiffrants commandé par l'automate de déverrouillage qui lui transmet les octets indiquant les numéros de page et les numéros de rangées des données transmises et le signal correspondant à la clé de service en cours (K), ce générateur d'octets déchiffrants possédant une sortie qui délivre, pour chaque octet chiffré reçu, un octet déchiffrant C_j

possédant un élément binaire de poids fort qui est forcé à zéro et des 7e et 6e éléments binaires nuls.

2. Système de vidéotex selon la revendication 1, caractérisé en ce que le générateur d'octets chiffrants du centre d'émission et le générateur d'octets déchiffrants des postes récepteurs comprennent chacun :

- un générateur de suite pseudo-aléatoire et un moyen pour réinitialiser ce générateur au début de chaque rangée visualisable, au moyen de la clé de service (K) et au moyen des numéros de page et de rangée,
- un circuit apte à prélever cinq éléments binaires à la sortie du générateur pseudo-aléatoire, ces cinq éléments constituant les cinq premiers éléments binaires de l'octet, et apte à ajouter des 6e et 7e éléments binaires qui sont nuls, et un 8e élément binaire qui est un élément de parité pour le générateur d'octets chiffrants et qui est forcé à zéro pour le générateur d'octets déchiffrants.

3. Système de vidéotex selon la revendication 2, caractérisé en ce que la clé de service est constituée par huit octets notés k_1 à k_8, et en ce que le numéro de rangée étant codé sur deux octets notés NR_1 et NR_2 et le numéro de page sur trois octets notés NP_1, NP_2 et NP_3, le générateur de suite pseudo-aléatoire est initialisé par huit octets obtenus par combinaison, à l'aide de la fonction logique OU-exclusif, des huit octets k_1 à k_8 respectivement avec huit octets pris parmi les octets NP_1, NP_2, NP_3, NR_1 et NR_2, ces combinaisons étant par exemple :

$k_1 \oplus NR_1$, $k_2 \oplus NR_2$, $k_3 \oplus NP_1$, $k_4 \oplus NP_2$, $k_5 \oplus NP_3$, $k_6 \oplus NP_3$, $k_7 \oplus NR_1$, $k_8 \oplus NR_2$.

4. Système de vidéotex selon la revendication 2, caractérisé en ce que le générateur de suite pseudo-aléatoire est constitué par un circuit comprenant des bascules de type (D) en cascade combinées à des portes

logiques de type OU-exclusif, ce circuit ayant une entrée reliée à une horloge et matérialisant un polynome générateur primitif.

5. Système de vidéotex selon la revendication 4, caractérisé en ce que le générateur de suite pseudo-aléatoire est constitué par plusieurs circuits matérialisant chacun un polynome générateur primitif, les sorties de ces circuits étant combinées par des circuits logiques.

6. Système de vidéotex selon l'une quelconque des revendications 1 à 4, caractérisé en ce qu'il comprend en outre :

A) - un centre de gestion d'abonnements (100) qui engendre des signaux numériques correspondant à des clés d'abonnement C_i, ces clés changeant de manière aléatoire à intervalles longs par rapport aux intervalles de changement de la clé de service (K),

B) - dans le centre d'émission :

- un circuit (102) de combinaison des signaux correspondant auxdites clés d'abonnement C_i et du signal correspondant à la clé de service (K), cette combinaison étant définie par un algorithme F_{C_i} (K) paramétré par les clés d'abonnement C_i, ce circuit délivrant autant de messages $M_i = F_{C_i}$ (K) qu'il y a de clés d'abonnements C_i, ces messages changeant avec la clé de service (K), l'ensemble des messages M_i étant organisé en une page spéciale dite page de contrôle d'accès, transmise cycliquement par l'organe d'émission, mais qui n'est pas visualisable,

C) - dans chaque poste récepteur :

- i) un support d'abonnement (106) muni d'une mémoire (108) contenant au moins une des clés d'abonnement C_i,
- j) un circuit (110) de restitution de la clé de service (K), recevant l'ensemble des

messages M_i constituant la page de contrôle d'accès, et d'autre part, la clé d'abonnement C_i ce circuit déroulant un algorithme $K = G_{C_i}(M_i)$ restituant le signal correspondant à la clé de service (K) employée dans le centre d'émission,

D) - au moins un poste (112) de chargement des supports d'abonnement, ce poste étant relié au centre de gestion d'abonnements d'où il reçoit les signaux correspondant aux différentes clés d'abonnement C_i engendrées par ce centre, chaque poste étant apte à recevoir temporairement des supports d'abonnement et à y inscrire durablement l'une des clés d'abonnement C_i.

7. Système de vidéotex selon la revendication 5, caractérisé en ce que le circuit (102) de formation des messages M_i par combinaison des signaux correspondant aux clés d'abonnement C_i avec le signal correspondant à la clé de service (K) comprend des moyens pour dérouler l'algorithme suivant :

- calculer un mot π de 61 éléments binaires engendrés au hasard,
- calculer l'inverse π^{-1} de π, modulo $2^{61}-1$,
- calculer le mot $\nu = K.\pi^{-1}$, modulo $2^{61}-1$,
- calculer le mot γ inverse de C_i, modulo $2^{127}-1$,
- calculer enfin le mot $M_i = \gamma(\nu + 2^{64}\pi)$, modulo $2^{127}-1$.

8. Système de vidéotex selon la revendication 7, caractérisé en ce que, dans le poste récepteur, le circuit (110) de restitution de la clé de service à partir des messages M_i et de la clé de service (K) est apte à dérouler l'algorithme suivant :

a) - un message M_i de 127 éléments binaires utiles, est saisi octet par octet, et une multiplication par C_i est effectuée pour former un mot μ :

$$\mu = M \cdot C \quad \text{modulo } (2^{127}-1)$$

les éléments binaires 1 à 61 de μ représentant un mot ν, tandis que les éléments binaires 65 à 125 représentent un mot π ;

b) - π et ν sont multipliés, modulo $2^{61}-1$, ce qui donne K.

9. Système de vidéotex selon la revendication 6, caractérisé en ce qu'il comprend, dans le centre d'émission, des moyens (124) aptes à constituer une page de contrôle d'accès avec :

- une rangée zéro qui comprend trois codes complémentaires C_1, C_2, C_3 indiquant qu'il s'agit d'une page de service non visualisable et un quatrième code complémentaire C_4 spécifiant qu'il s'agit d'une page de contrôle d'accès,
- des rangées constituées par un en-tête de rangée suivi d'un numéro de rangée, suivi d'un bloc d'accès constitué par un message M_i suivi d'un code de redondance cyclique.

10. Système de vidéotex selon la revendication 6, caractérisé en ce que les signaux numériques d'abonnement sont des blocs composés de quatre champs :

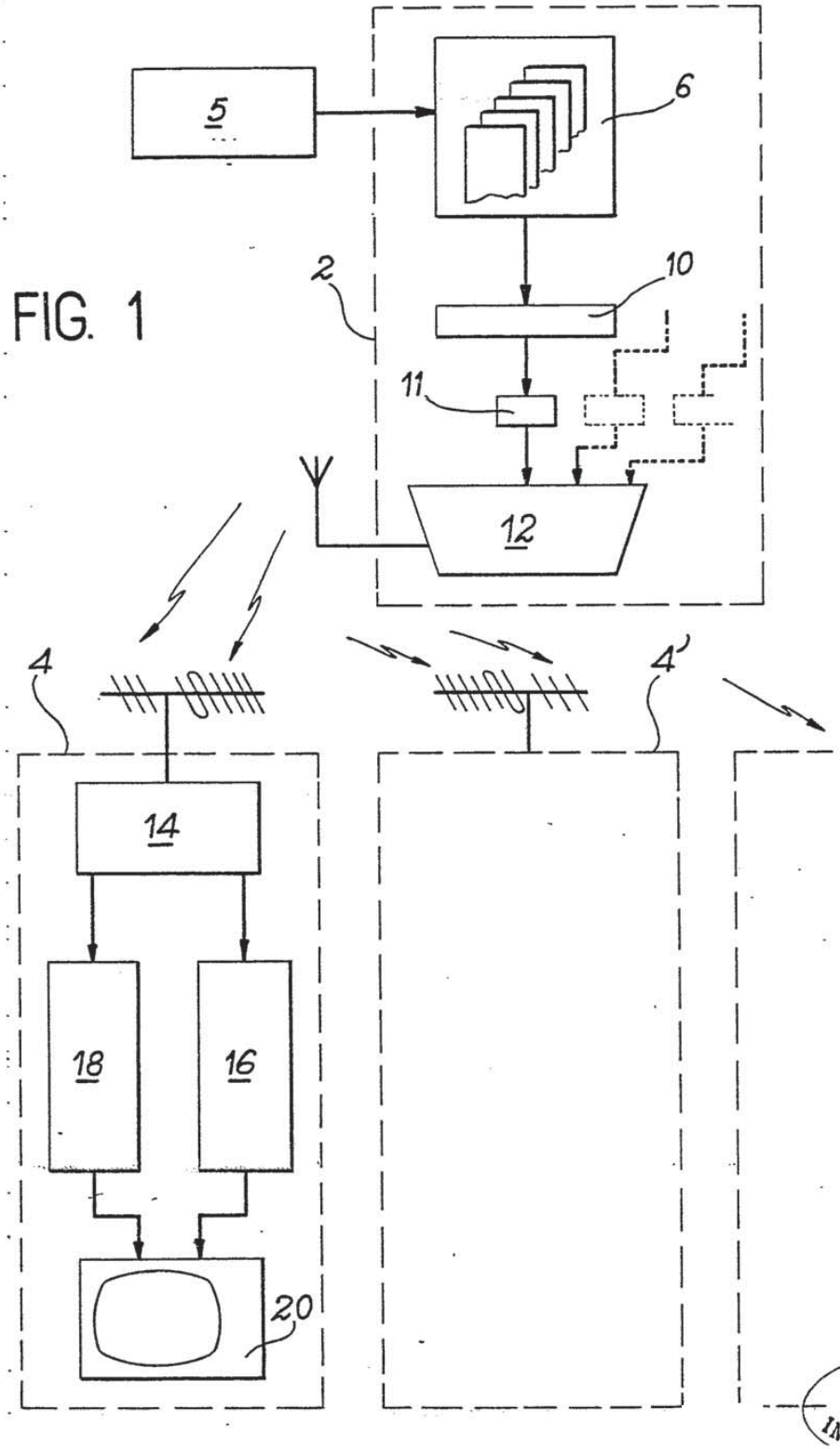
- un code de service,
- un indice d'abonnement (sur 8 éléments binaires),
- une clé d'abonnement,
- un code de redondance cyclique.

11. Système de vidéotex selon les revendications 9 et 10, caractérisé en ce que l'indice d'abonnement est pris comme numéro de rangées dans la page de contrôle d'accès.

12. Système de vidéotex selon l'une quelconque des revendications 1 à 11, caractérisé en ce qu'il est conforme au système ANTIOPE.

13. Système de vidéotex selon l'une quelconque des revendications 1 à 11, caractérisé en ce qu'il est conforme au système TITAN.

FIG. 1



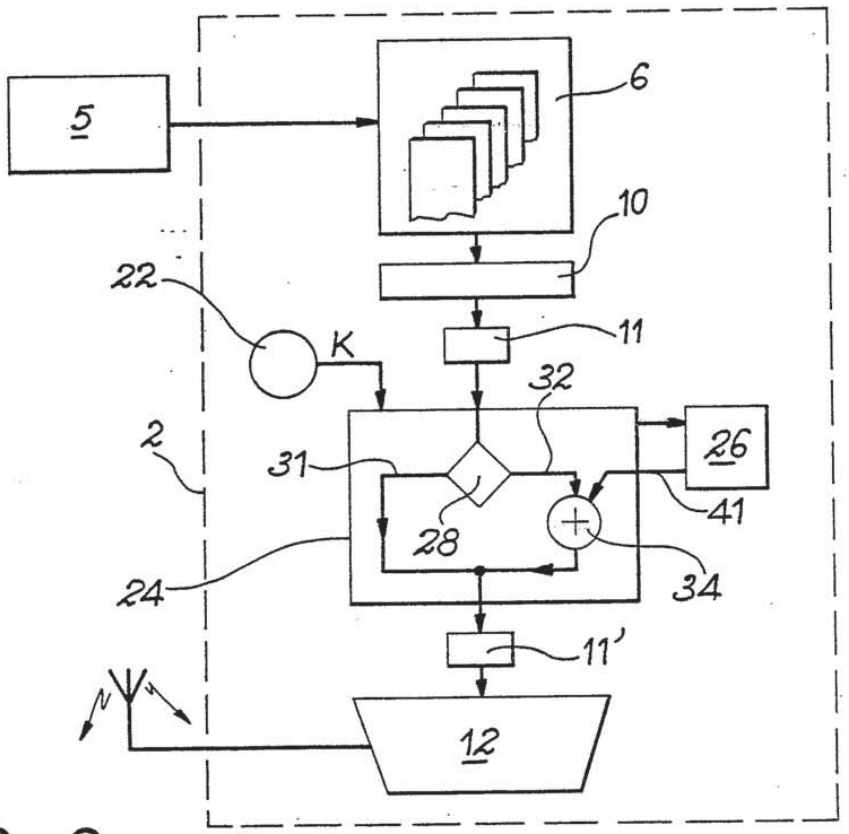
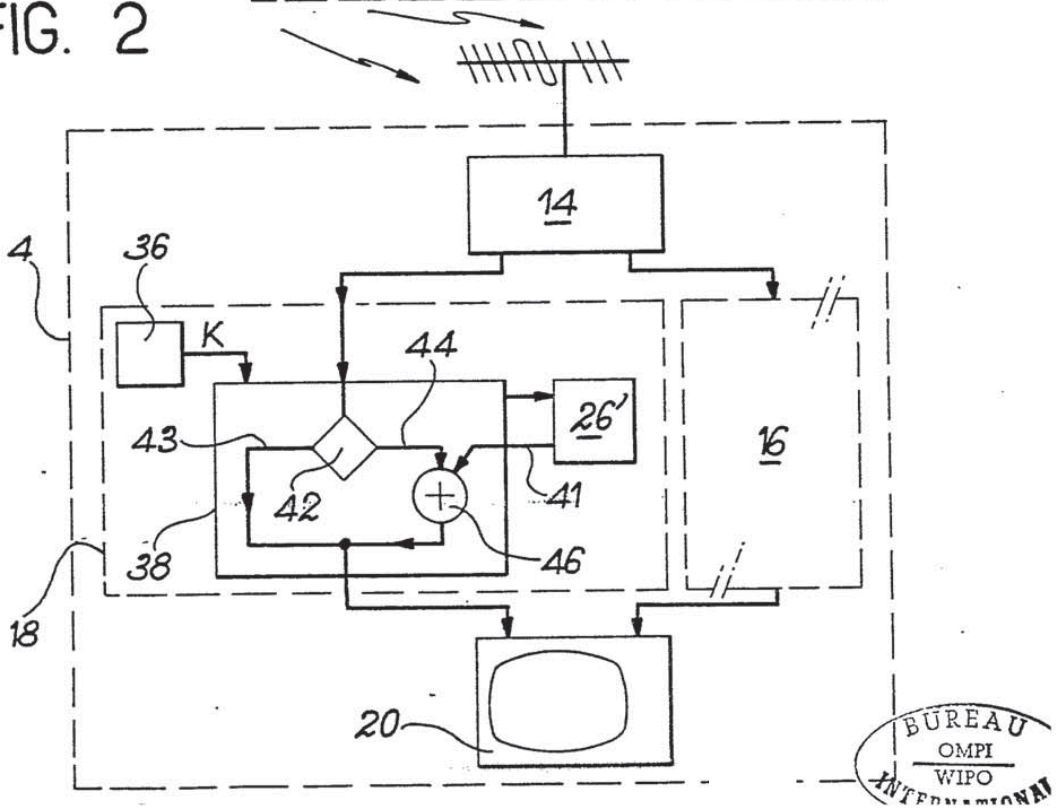


FIG. 2



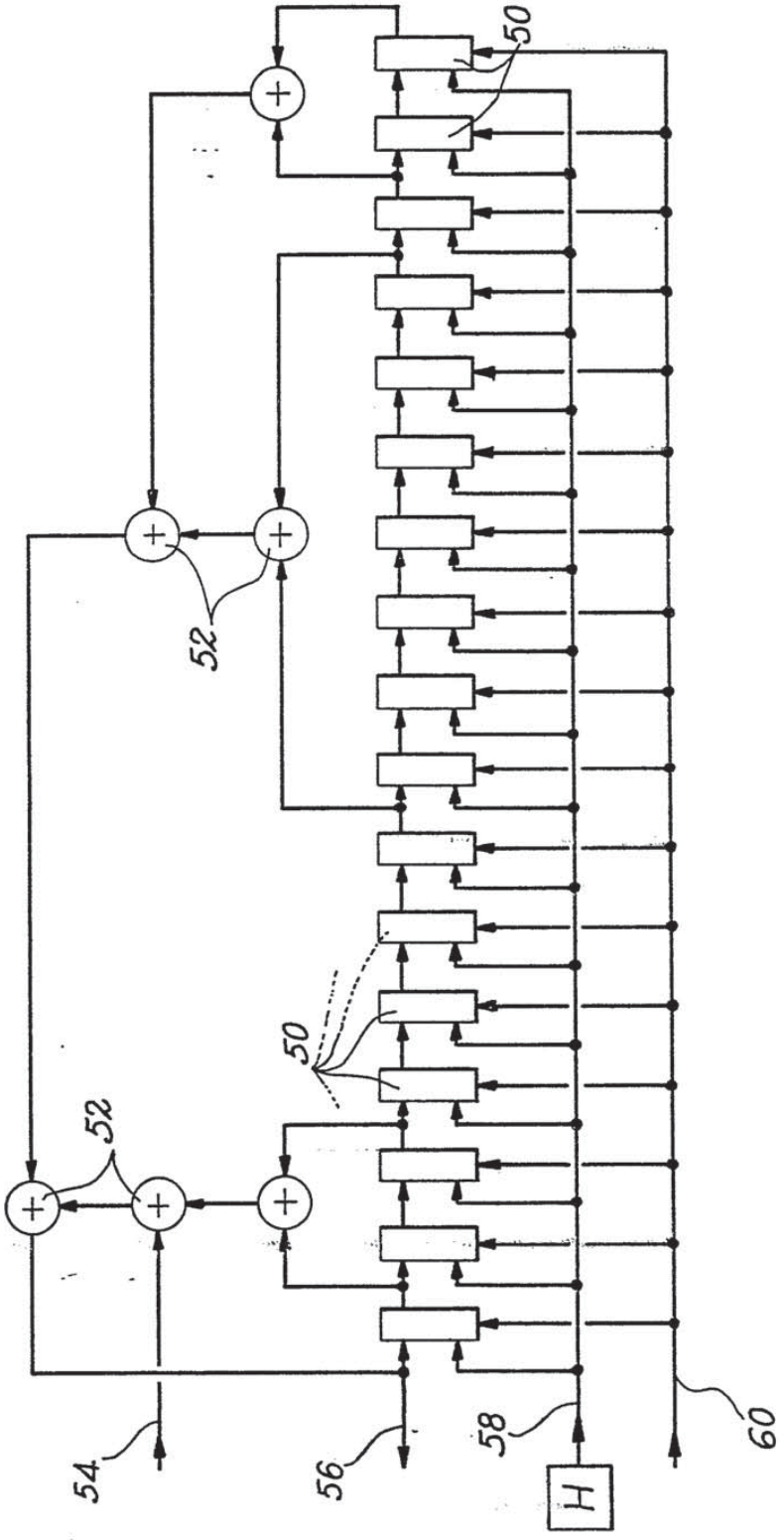


FIG. 3

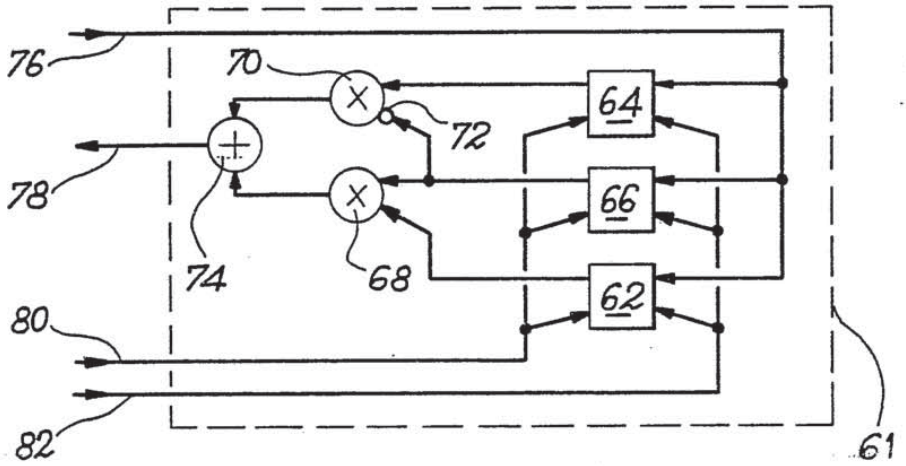


FIG. 4

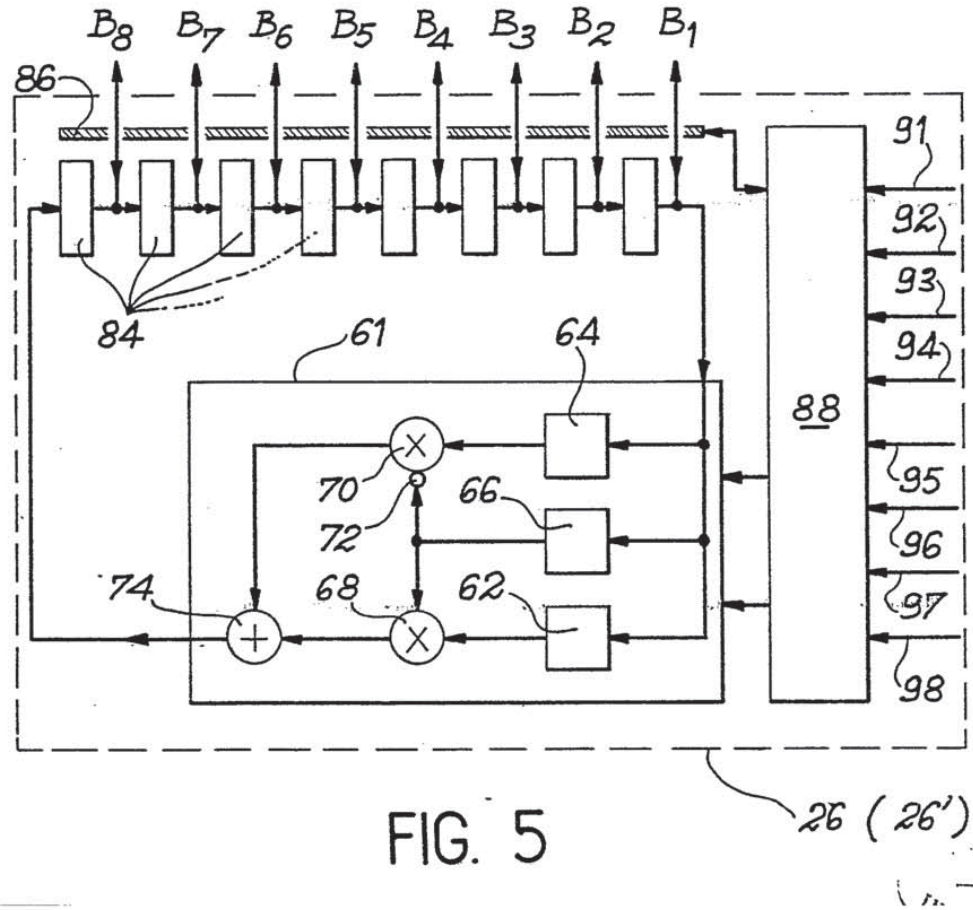


FIG. 5

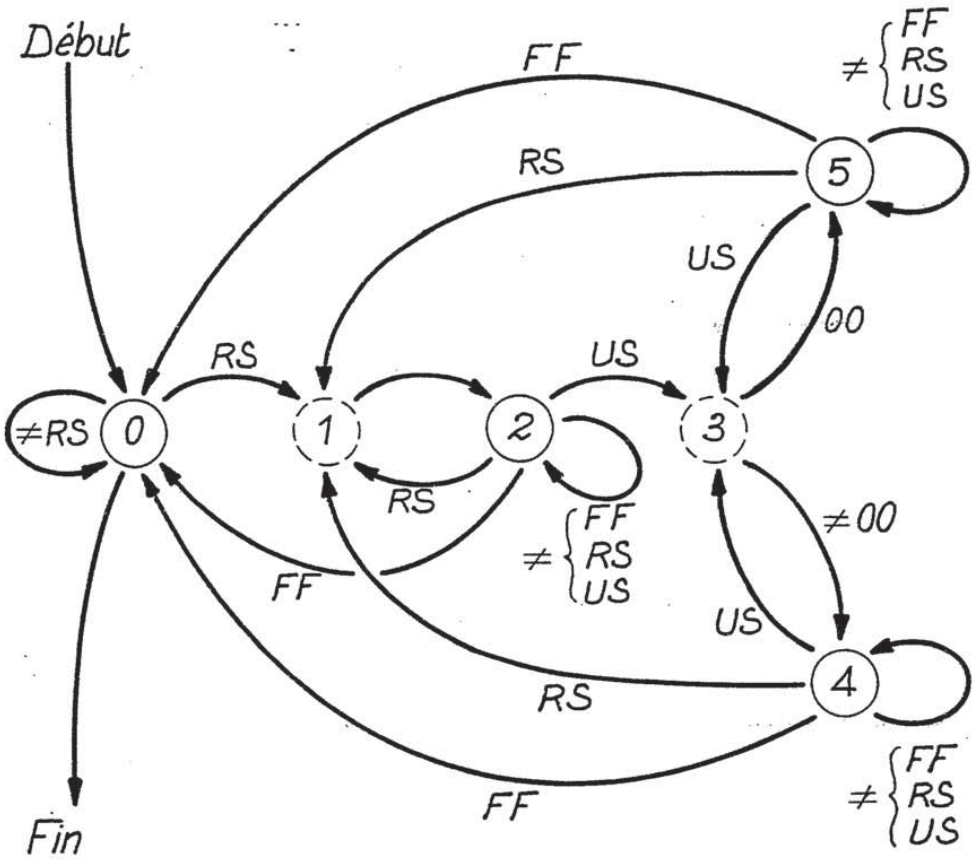


FIG. 6

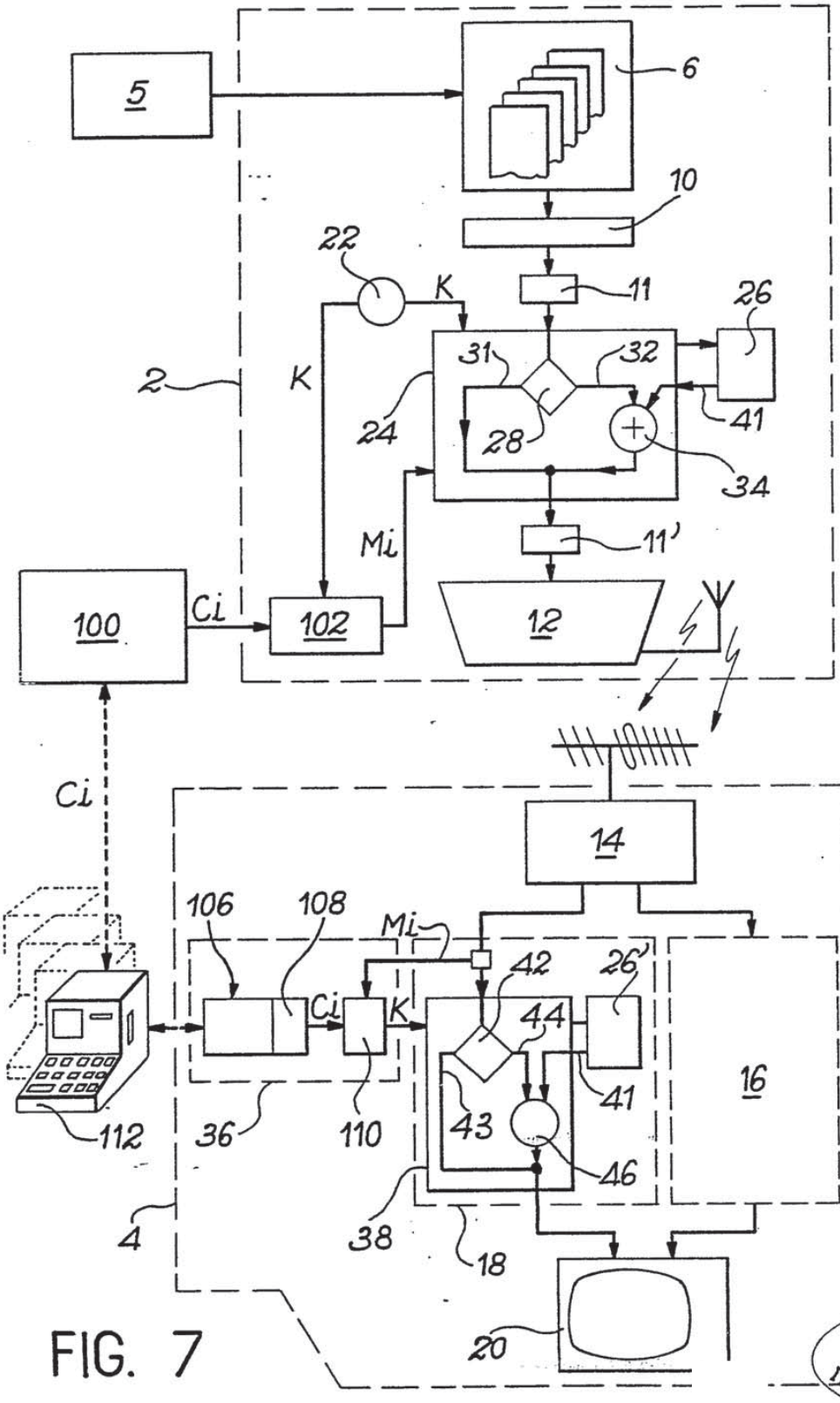


FIG. 7

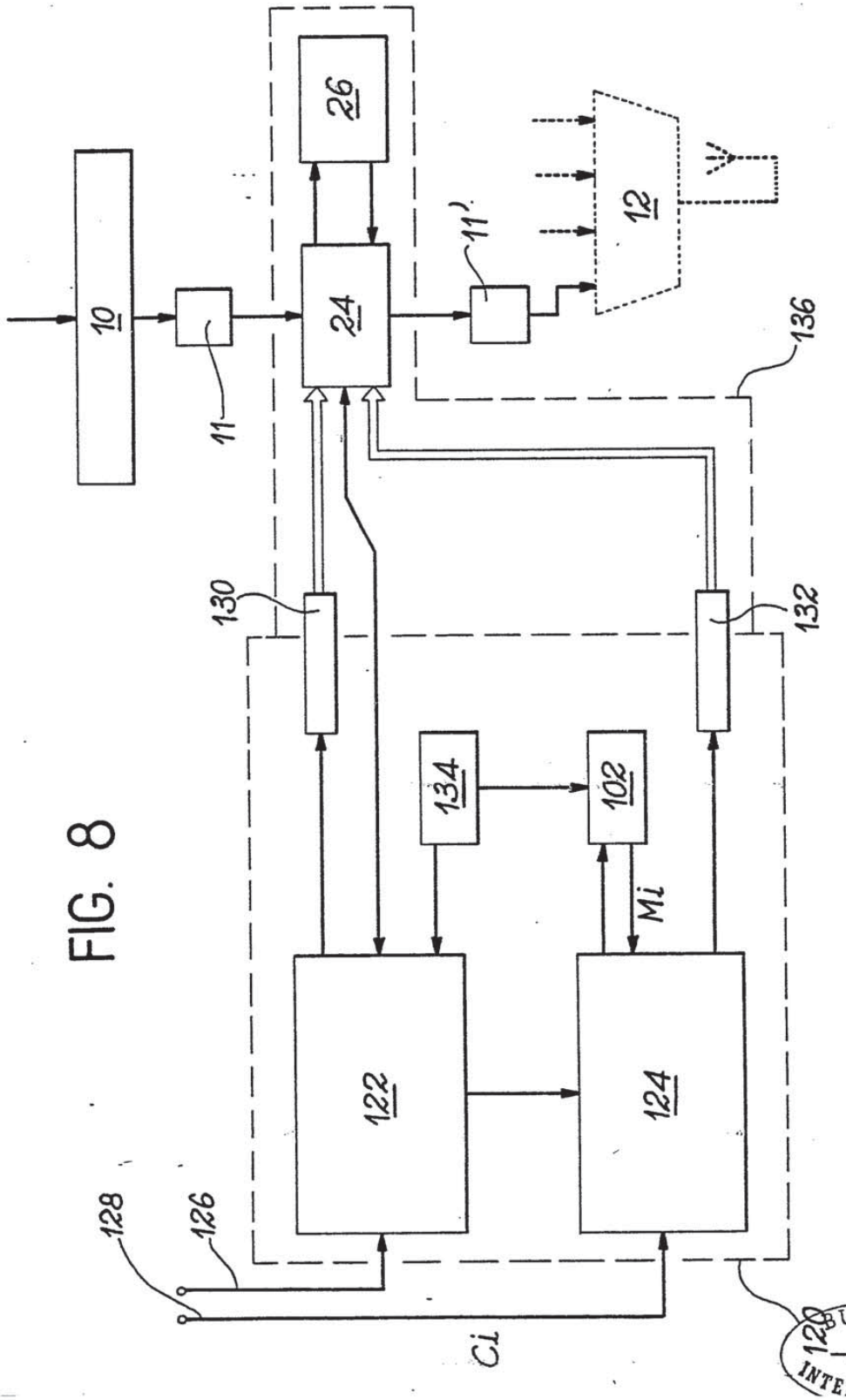


FIG. 8

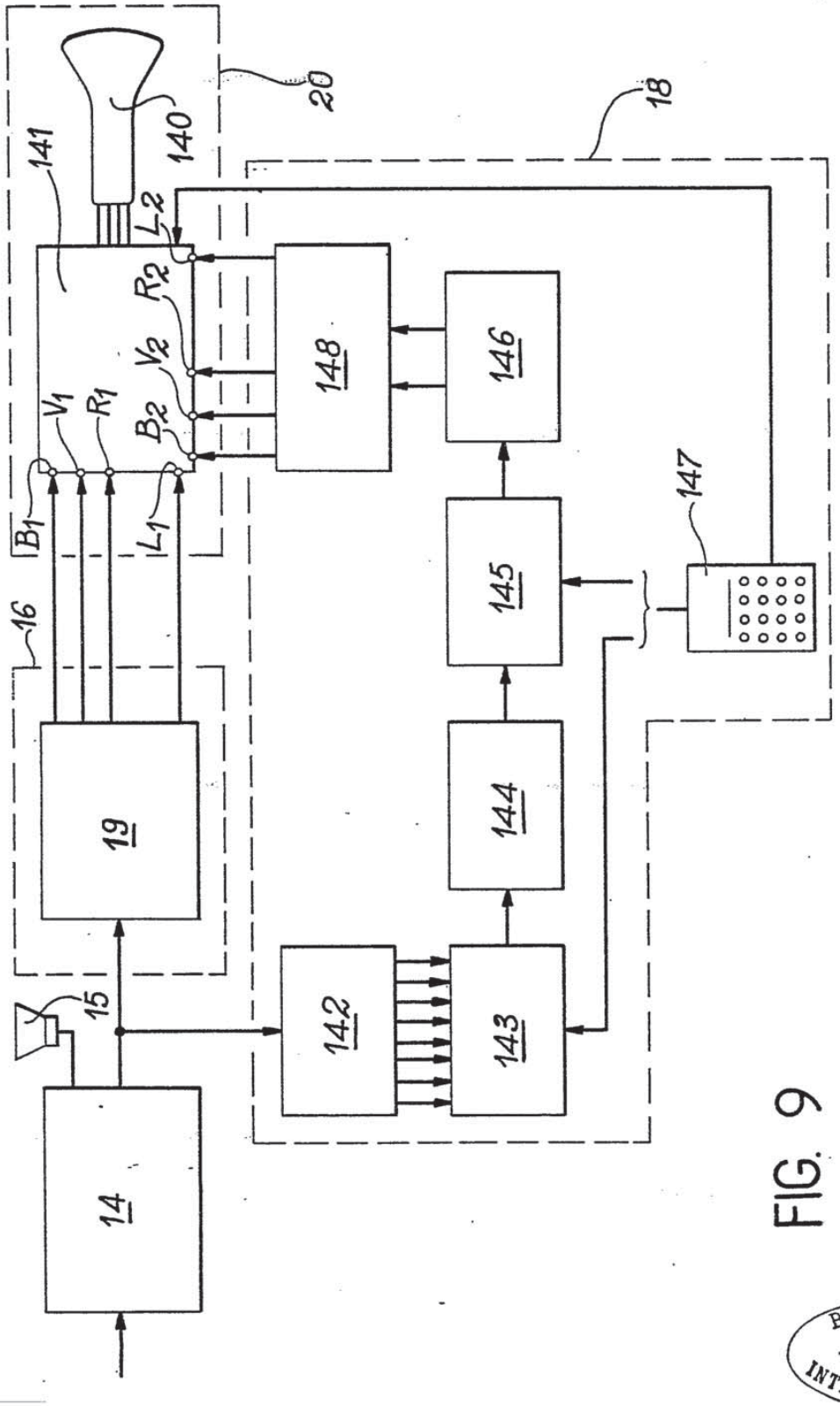


FIG. 9

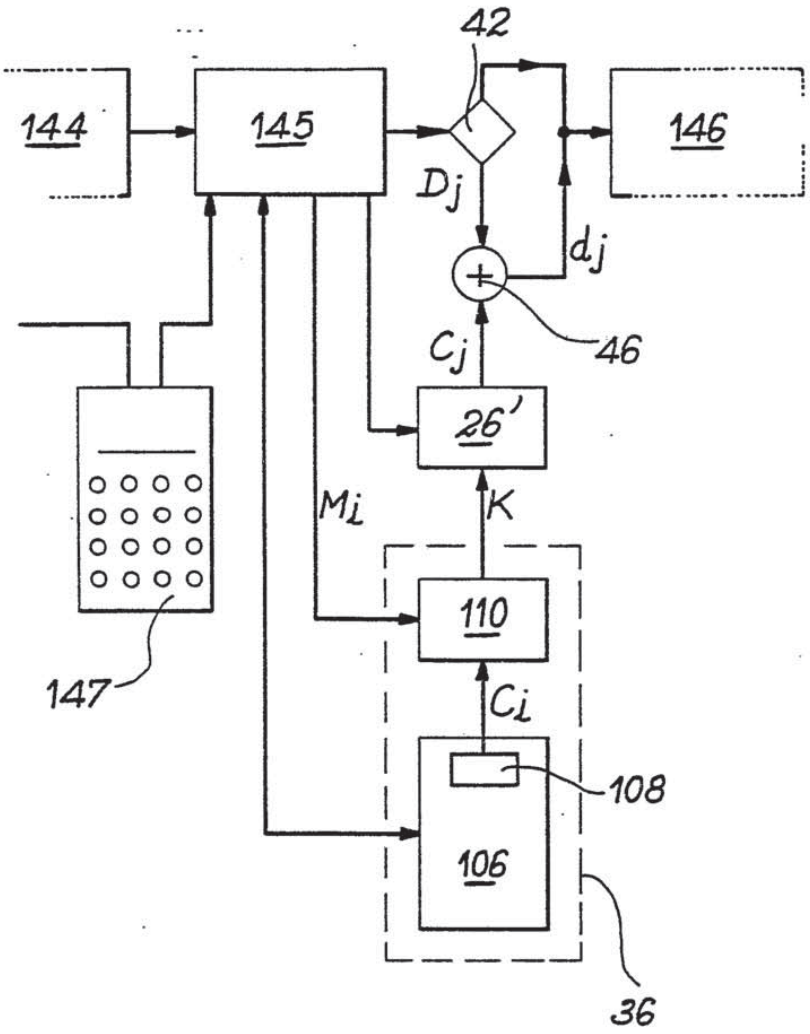


FIG. 10

RAPPORT DE RECHERCHE INTERNATIONALE

Demande internationale N° PCT/FR 80/00019

I. CLASSEMENT DE L'INVENTION (si plusieurs symboles de classification sont applicables, les indiquer tous) [3]

Selon la classification internationale des brevets (CIB) ou à la fois selon la classification nationale et la CIB

Int.Cl.[3] H 04 N 7/16

II. DOMAINES SUR LESQUELS LA RECHERCHE A PORTÉ

Documentation minimale consultée [4]

Système de classification	Symboles de classification
Int.Cl.[3]	H 04 N 7/16; H 04 N 7/04

Documentation consultée autre que la documentation minimale dans la mesure où de tels documents font partie des domaines sur lesquels la recherche a porté [5]

III. DOCUMENTS CONSIDÉRÉS COMME PERTINENTS [14]

Catégorie *	Identification des documents cités,[16] avec indication, si nécessaire, des passages pertinents [17]	N° des revendications visées [18]
	FR, A, 2316821, publié le 28 janvier 1977 voir page 1, lignes 1 à 26; page 3, ligne 13 à page 5, ligne 28, Dynamic Technology LTD	1,2,4,12
	--	
	FR, A, 2117478, publié le 21 juillet 1972 voir page 3, ligne 4 à page 9, ligne 21, Gretag A.G.	6
	------	

* Catégories spéciales de documents cités: [15]

«A» document définissant l'état général de la technique

«E» document antérieur, mais publié à la date de dépôt international ou après cette date

«L» document cité pour raison spéciale autre que celles qui sont mentionnées dans les autres catégories

«O» document se référant à une divulgation orale, à un usage, à une exposition ou tous autres moyens

«P» document publié avant la date de dépôt international mais à la date de priorité revendiquée ou après celle-ci

«T» document ultérieur publié à la date de dépôt international ou à la date de priorité, ou après, et n'appartenant pas à l'état de la technique pertinent, mais cité pour comprendre le principe ou la théorie constituant la base de l'invention

«X» document particulièrement pertinent

IV. CERTIFICATION

Date à laquelle la recherche internationale a été effectivement achevée [2]	Date d'expédition du présent rapport de recherche internationale [2]
14 mai 1980	23 mai 1980
Administration chargée de la recherche internationale [1]	**Signature du fonctionnaire autorisé [20]**
Office Européen des Brevets	G.L.M. Kruydenberg

Formulaire PCT/ISA/210 (deuxième feuille) (Octobre 1977)

INTERNATIONAL SEARCH REPORT

International Application No PCT/FR80/00019

I. CLASSIFICATION OF SUBJECT MATTER (if several classification symbols apply, indicate all) [3]

According to International Patent Classification (IPC) or to both National Classification and IPC

Int.Cl.[3] H 04 N 7/16

II. FIELDS SEARCHED

Minimum Documentation Searched [4]

Classification System	Classification Symbols
Int.Cl.[3]	H 04 N 7/16; H 04 N 7/04

Documentation Searched other than Minimum Documentation to the Extent that such Documents are Included in the Fields Searched [5]

III. DOCUMENTS CONSIDERED TO BE RELEVANT [14]

Category *	Citation of Document, [16] with indication, where appropriate, of the relevant passages [17]	Relevant to Claim No. [18]
	FR, A, 2316821, published on 28 January 1977, see page 1, lines 1 to 26; page 3, line 13 to page 5, line 28, Dynamic Technology LTD	1,2,4,12
	FR, A, 2117478, published on 21 July 1972 see page 3, line 4 to page 9, line 21, Gretag A.G.	6

* Special categories of cited documents: [15]

"A" document defining the general state of the art

"E" earlier document but published on or after the international filing date

"L" document cited for special reason other than those referred to in the other categories

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but on or after the priority date claimed

"T" later document published on or after the international filing date or priority date and not in conflict with the application, but cited to understand the principle or theory underlying the invention

"X" document of particular relevance

IV. CERTIFICATION

Date of the Actual Completion of the International Search [2]	Date of Mailing of this International Search Report [2]
14 May 1980 (14.05.80)	23 May 1980 (23.05.80)
International Searching Authority [1]	**Signature of Authorized Officer [20]**
EUROPEAN PATENT OFFICE	

Form PCT/ISA/210 (second sheet) (October 1977)