(19) RÉPUBLIQUE FRANÇAISE

INSTITUT NATIONAL
DE LA PROPRIÉTÉ INDUSTRIELLE

PARIS

(11) N° de publication : **2 583 946**
(à n'utiliser que pour les commandes de reproduction)

(21) N° d'enregistrement national : **85 09679**

(51) Int Cl⁴ : H 04 N 7/167.

(12) DEMANDE DE BREVET D'INVENTION A1

(22) **Date de dépôt :** 24 juin 1985.

(30) **Priorité :**

(43) **Date de la mise à disposition du public de la demande :** BOPI « Brevets » n° 52 du 26 décembre 1986.

(60) **Références à d'autres documents nationaux apparentés :**

(71) **Demandeur(s) :** *L'ETAT Français représenté par le Ministre des P.T.T. (Centre National des Télécommunications) CNET et Etablissement Public de Diffusion dit « Télédiffusion de France).* — FR.

(72) **Inventeur(s) :** Jean, François Gautier Christian

(73) **Titulaire(s) :**

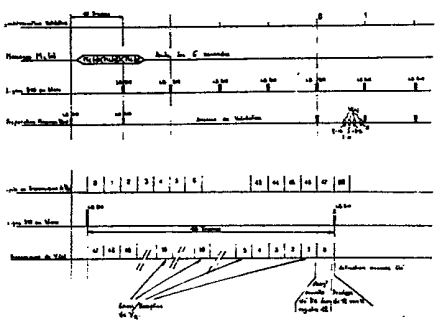
(74) **Mandataire(s) :** Cabinet Louis Le Guen.

(54) Système de télévision à contrôle d'accès utilisant une clé électronique variable.

(57) Le système permet d'embrouiller l'information à l'émission et de la désembrouiller à la réception à l'aide d'une clé (K(*n*)).

La transmission de la clé (K(*n*)) de l'émetteur aux récepteurs est effectuée d'une manière connue quelconque. En plus de la clé, est transmis un signal de validation (V(*n*)) de clé. Chaque clé K(*n*)) est déterminée, dans chaque récepteur, à partir d'un message ($M_i(n)$) transmis par l'émetteur et une clé d'abonnement C_i. Chaque message ($M_i(n)$) est répété plusieurs fois successivement à intervalles réguliers. Les différentes clés ($M_i(n)$) contiennent une information *n* qui identifie leur rang, chaque signal (V(*n*)) contenant également l'information *n* permettant d'identifier la clé (K(*n*)) à utiliser.

Chaque signal de validation V(*n*) est transmis plusieurs fois dans des trames prédéterminées et à des intervalles de temps prédéterminés avant chaque validation de clé, la dernière transmission étant effectuée dans la trame qui précède le changement effectif de clé.



FR 2 583 946 - A1

Vente des fascicules à l'IMPRIMERIE NATIONALE, 27, rue de la Convention — 75732 PARIS CEDEX 15

La présente invention concerne un système de télévision à contrôle d'accès utilisant une clé électronique variable.

De tels systèmes ont déjà été décrits dans les documents FR-A-2 448 824, FR-A-2 448 825, FR-A-2 448 826 et FR-A-2 459 595. En particulier, dans le système décrit dans le brevet FR-A-2 459 595, on prévoit d'utiliser un système à double clé, c'est-à-dire une clé de service K qui permet d'embrouiller l'information et qui change de manière aléatoire à des intervalles relativement courts, de l'ordre de quelques minutes, et une clé d'abonnement pouvant prendre plusieurs valeurs C_i selon le type d'abonnement. La clé C_i change de manière aléatoire à des intervalles relativement longs, de l'ordre du mois, et est inscrite sur un support d'abonnement introduit dans chaque poste récepteur du système. Les deux clés K et C_i sont combinées à l'émission pour constituer des messages M_i qui sont transmis de l'émetteur aux récepteurs. La transmission des messages M_i s'effectue selon la procédure DIDON, ce qui confère au système une compatibilité avec les services numériques déjà existants et basés sur cette procédure, comme par exemple les services de télétexte tels que le télétexte "Antiope". A la réception, les messages M_i reçus sont combinés avec la clé d'abonnement C_i du support d'abonnement que l'abonné a introduit dans son poste récepteur afin de restituer la clé K nécessaire au débrouillage du signal d'image embrouillé reçu.

A titre indicatif, la procédure DIDON est définie dans les brevets FR-A-2 313 825, FR-A-2 393 480 et FR-A-2 404 350. Egalement à titre indicatif, le service de télétexte ANTIOPE (marque déposée) est défini dans les brevets FR-A-2 363 843, FR-A-2 363 949 et FR-A-2 419 623. Enfin, toujours à titre indicatif, des systèmes d'embrouillage et de désembrouillage d'images de télévision sont décrits dans les brevets FR-A-2 230 236 et FR-A-2 431 809.

Dans le système décrit dans le brevet FR-2 459 595, à chaque changement de clé K, le message M_i permettant aux récepteurs de calculer la nouvelle clé est transmis un peu avant la trame à laquelle sera affectée la nouvelle clé. Dans chaque récepteur, le calcul de la nouvelle clé K à partir de C_i et M_i prend un certain temps. Comme le réseau DIDON transmet des informations provenant de plusieurs voies, lesquelles sont en concurrence, un décalage de temps indéterminé existe entre l'instant de demande de transmission du message M_i et l'instant de sa transmission. Il est donc nécessaire de

faire connaître au récepteur à quelle trame la clé aura effectivement changé. C'est pourquoi, dans le brevet FR-A-2 459 595, il est prévu de transmettre un signal de marquage qui est inséré dans le signal vidéo de la trame qui précède celle du changement de clé. Ce signal peut avoir la forme d'une impulsion, telle que la mise au blanc d'une ligne non visible. Comme la transmission du message M_i peut être retardée, vu le trafic sur le réseau DIDON, il peut arriver que le calcul de K dans les récepteurs ne soit pas encore terminé alors que le signal de ligne au blanc est reçu. Le traitement de l'image s'effectue alors avec une fausse clé sans réel désembrouillage.

Dans le service ANTIOPE, on sait que les problèmes de synchronisation trouvent leur solution dans l'envoi séquentiel des données de programme et des données de contrôle d'accès s'y rapportant. Les informations de chiffrement sont regroupées dans un article de contrôle d'accès qui est diffusé cycliquement et remis à jour à chaque changement de clé. Le synchronisme d'application d'une nouvelle clé est réalisé par l'introduction d'un nouvel article de contrôle d'accès.

Il peut également arriver que la détection de la ligne au blanc soit perturbée par des parasites, ce qui entraîne de continuer à utiliser trop longtemps la clé antérieure, qui est alors fausse.

Un objet de la présente invention consiste à prévoir un système de télévision à contrôle d'accès qui évite les inconvénients mentionnés ci-dessus et notamment le déclenchement prématuré ou trop tardif d'un changement de clé.

Suivant une caractéristique de l'invention, en plus du message M_i transmis par le réseau DIDON, il est transmis également par le réseau DIDON un signal de validation de changement de clé.

Suivant une autre caractéristique de l'invention, différents messages $M_i(n)$ contenant une information $\underline{n}$ qui identifie le rang du message, peuvent être transmis successivement, entraînant à chaque fois le calcul d'une nouvelle clé K(n) qui est mémorisée, le signal V(n) de validation de changement de clé contenant également l'information $\underline{n}$ permettant d'identifier et de rechercher en mémoire la clé K(n) à utiliser.

Dans le système suivant l'invention, seule la voie DIDON portant les signaux de validation doit garder pendant la transmission

une relation de phase définie avec les images embrouillées. Par contre, la voie portant les messages $M_i(n)$ peut n'avoir aucune relation de phase avec le programme des clés. Seul un temps nécessaire au transit de l'information et au calcul de chaque clé doit être pris en compte. Dans ce système, on peut utiliser plusieurs articles de contrôle d'accès vers les terminaux qui calculent les clés correspondantes et les mémorisent, les clés calculées n'étant activées qu'au fur et à mesure que le signal de validation V(n) y afférant sera émis.

Suivant une autre caractéristique, chaque message $M_i(n)$ est répété plusieurs fois à intervalles réguliers, par exemple trois fois et toutes les six secondes.

Suivant une autre caractéristique, chaque signal de validation V(n) est transmis plusieurs fois dans des trames prédéterminées et à des intervalles de temps prédéterminés avant chaque validation de clé, la dernière transmission étant effectuée dans la trame qui précède le changement effectif de clé.

Suivant une autre caractéristique, toutes les $\underline{x}$ trames, avec $\underline{x}$ égal à 48 par exemple, est transmis un signal de synchronisation de cycle de $\underline{x}$ trames qui provoque le chargement de la clé déjà validée.

Suivant une autre caractéristique, un nombre prédéterminé de signaux successifs de synchronisation de cycle de $\underline{x}$ trames est supprimé avant chaque transmission de signal de validation V(n), le premier signal de synchronisation de cycle de $\underline{x}$ trames réapparaissant indiquant que le signal de validation ou la série de signaux de validation V(n) va être transmis dans le groupe de $\underline{x}$ trames suivant.

Les caractéristiques de l'invention mentionnées ci-dessus, ainsi que d'autres, apparaîtront plus clairement à la lecture de la description suivante d'un exemple de réalisation, ladite description étant faite en relation avec les dessins joints, parmi lesquels:

la Fig. 1 est un bloc-diagramme de la partie émission des messages $M_i(n)$ et V(n),

la Fig. 2 est le bloc-diagramme de la partie réception de ces messages,

la Fig. 3 est le bloc-diagramme du circuit d'embrouillage utilisé dans la partie émission de la Fig. 1,

la Fig. 4 est le bloc-diagramme de l'unité de commande de la partie émission de la Fig. 1,

la Fig. 5 est le bloc-diagramme du circuit de génération des messages $M_i(n)$ et V(n) dans la partie émission de la Fig. 1,

les Figs. 6a à 6d sont des diagrammes temporels illustrant les signaux émis par la partie émission de la Fig. 1,

les Figs. 7a à 7e et 8a à 8d sont des diagrammes temporels illustrant le chargement de clé, et

la Fig. 9 est le bloc-diagramme du désembrouilleur du récepteur de la Fig. 2.

Dans la partie émission de la Fig. 1, on a regroupé les différents circuits en quatre blocs: un circuit d'embrouillage ou embrouilleur 1, un multiplexeur 2, un générateur de message 3 et une unité de commande 4.

L'embrouilleur 1, Fig. 3, comprend un générateur de séquence numérique pseudo-aléatoire 11, un registre de chargement 12, un circuit séparateur de synchronisations ligne et trame 13, un convertisseur analogique-numérique 14, un circuit de traitement du signal vidéo 15, un convertisseur numérique-analogique 16, un compteur 17, des multiplexeurs 18 à 22 et un inverseur 23.

D'une manière générale, le circuit d'embrouillage 1 fontionne comme le circuit qui est montré à la Fig. 2 du brevet FR-A-2 459 595. On rappelle que, dans le signal de télévision, les lignes de suppression trame ne sont pas embrouillées, de même que dans chaque ligne, l'intervalle de suppression ligne. Certaines des lignes de l'intervalle de suppression trame sont utilisées pour transmettre chacune un paquet de service DIDON. De plus, toujours dans l'intervalle de suppression trame, la ligne 310 peut être mise au niveau du blanc pour marquer un instant bien précis dans la trame dont elle fait partie. Les Figs. 6a à 6c illustrent respectivement la position de la ligne 310, l'intervalle de suppression trame et le signal de synchronisation trame. La Fig. 6d montre les vingt lignes qui suivent les lignes d'égalisation de la synchronisation trame et qui servent à transmettre chaque clé K(n) du registre de chargement 12 au générateur de séquence pseudo-aléatoire 11, comme on le verra dans la suite. Le signal de la Fig. 6d sera dans la suite appelé "fenêtre de chargement".

Le circuit séparateur de synchronisations ligne et trame 13 reçoit, par le câble 24, le signal vidéo normal d'où il extrait le

signal de synchronisation ligne SYNC L qui lui permet, à l'aide de compteurs, de fonctionner comme une base de temps à l'égard des autres circuits. Le circuit 13 a également une sortie SYNC T par laquelle est délivré le signal de la synchronisation trame de la Fig. 6c. La sortie SYNC L est reliée à l'entrée du compteur 17 dont l'entrée de remise à zéro est reliée à la sortie SYNC T. Le compteur 17 a une capacité de 310 et sa sortie délivre le signal de la Fig. 6a. Enfin, le circuit 13 a une troisième sortie SUPP T qui délivre le signal de la Fig. 6b, c'est-à-dire le signal de suppression trame.

Le registre de chargement 12 sert de mémoire pour chaque clé K. Son entrée de données est reliée à la sortie du multiplexeur à deux entrées 19 dont une entrée est reliée à la sortie du registre 12 et dont l'autre entrée est reliée à l'unité de commande 4 par un fil 25. L'entrée de commande du multiplexeur 19 est également reliée à l'unité de commande 4 par un fil 26 qui est actif pendant la fenêtre de chargement. Enfin, l'entrée d'horloge du registre 12 est reliée à la sortie du multiplexeur à deux entrées 18 dont une entrée est reliée à la sortie SYNC L et l'autre à l'unité de commande 4 par un fil 27 qui transmet l'horloge de la transmission des données sur le fil 25. Les signaux d'horloge transmis sur le fil 25 sont engendrés dans le microprocesseur de l'unité de commande 4.

Le générateur de séquence pseudo-aléatoire 11 est, par exemple, un registre à décalage à vingt étages pourvu d'un certain nombre de points de rebouclage, dont le rebouclage direct entre le dernier et le premier étage. Les bouclages intermédiaires sont activés quand un niveau "1" est appliqué à l'entrée de commande de l'étage correspondant. Ces niveaux de commande sont appliqués à partir du registre de chargement 12. Le générateur 11 a son entrée de données reliée à la sortie du multiplexeur 20 dont une entrée est reliée à la sortie série de 11 et l'autre à la sortie série de 12. L'entrée de commande du multiplexeur 20 est reliée à la sortie de l'inverseur 23 dont l'entrée est reliée au fil 26. L'entrée d'horloge du registre 11 est reliée à la sortie SYNC L du circuit 13.

Le convertisseur analogique-numérique 14 effectue la numérisation des signaux vidéo des lignes à embrouiller reçus du câble 24. Le circuit de traitement 15 effectue sur le signal numérisé que lui

transmet le convertisseur 14, les décalages, les permutations et/ou les retournements de segments et les inversions de polarité en fonction du mot parallèle délivré, sur 28, par le générateur de séquence aléatoire 11. On pourra, au sujet de ce traitement, se reporter aux brevets FR-A-2 230 236 et FR-A-2 431 809 déjà cités.

Le multiplexeur à deux entrées 21 a sa sortie reliée au multiplexeur 22, son entrée de commande reliée à la sortie SUPP T du circuit 13, une entrée de signal reliée à la sortie du convertisseur analogique-numérique 14 et son autre entrée de signal reliée à la sortie du circuit de traitement 15. La première entrée permet de transmettre le signal de suppression trame sans embrouillage au multiplexeur 22 et la seconde entrée transmet le reste des signaux embrouillés de la trame.

Le multiplexeur 22 a deux entrées, l'une reliée à la sortie du multiplexeur 21, l'autre reliée à la sortie d'une mémoire 30 qui contient une information de ligne au blanc, soit par exemple un octet avec les huit bits à "1". Son entrée de commande est reliée par un fil 29 à une sortie de l'unité de commande 4. Quand le fil 29 n'est pas activé, le multiplexeur 22 transmet les signaux de toutes les lignes fournis par le multiplexeur 21. Quand le fil 29 est activé, au moment de la transmission de la ligne 310, le multiplexeur 22 transmet le contenu de 30, le reste des lignes n'étant pas affecté. La sortie du multiplexeur 22 est reliée à l'entrée du convertisseur numérique-analogique 16.

La sortie du convertisseur 16 est reliée au fil 36 sur lequel elle transmet les signaux analogiques embrouillés.

Le générateur de message 3 comprend un circuit de gestion 31, un générateur de messages $M_i(n)$ 32 et un générateur de mots de validation V(n) 33. Le générateur 32 délivre les messages $M_i(n)$ sous la forme d'un paquet se décomposant en l'information M_i et l'information n. Ce paquet est transmis au multiplexeur 2 par la voie 34 et le multiplexeur 2 lui ajoute son en-tête de paquet. Le générateur 33 délivre les mots de validation qui se décomposent en une information V et l'information n. Ces mots de validation sont transmis sous forme de paquets par la voie 35 au multiplexeur qui lui ajoute son en-tête. Dans chaque en-tête, l'octet d'identification de voie indique au récepteur si l'information provient du générateur 32 ou du générateur

33. On verra plus en détail dans la suite le rôle du circuit de gestion 31.

Le multiplexeur 2 est un coupleur de réseau DIDON dont l'entrée vidéo est reliée à la sortie de l'embrouilleur 1, c'est-à-dire à la sortie du multiplexeur 22, par un câble 36. Il transmet cette vidéo embrouillée, plus, sur certaines lignes de l'intervalle de suppression trame, des paquets provenant notamment des générateurs 32 et 33. La sortie du multiplexeur 2 est reliée à un émetteur, non montré, par un câble 37, lequel comporte une dérivation 38 vers l'unité de commande 4. Un coupleur de réseau DIDON est décrit dans le document 3.80 de la revue "radiodiffusion-télévision".

L'unité de commande 4 comprend un démodulateur DIDON 40, un démultiplexeur DIDON 41, un microprocesseur 42, une carte d'accès 43 et un compteur 44.

Le démodulateur 40 permet de recevoir les données DIDON transmises sur la dérivation 38. Sa sortie est reliée à l'entrée du démultiplexeur 41 qui a deux entrées de commande reliées au microprocesseur 42 par les fils 45 et 46 qui commutent le démultiplexeur 41, l'un, 45, pour qu'il transmette les données $M_i(n)$ en reconnaissant l'en-tête de la voie 34, et l'autre, 46, pour qu'il transmette les données V(n) quand il reconnaît l'en-tête de la voie 35. La sortie du démultiplexeur 41 est reliée par le faisceau 47 à l'entrée de données du microprocesseur 42.

La carte d'accès 43 comprend une mémoire qui contient une valeur C_i et un microprocesseur. La liaison, par connecteur, entre la carte 43 et le microprocesseur 42 permet à ce dernier de transmettre à la carte 43 chaque message $M_i(n)$ qu'il reçoit. La carte 43 connaissant C_i et $M_i(n)$ fait calculer par son propre microprocesseur, selon son propre algorithme, la clé K(n) correspondante, puis la transmet au microprocesseur 42 qui la garde en mémoire à une adresse associée à n. Quand le microprocesseur reçoit le mot V(n), toujours du démultiplexeur 41, il en déduit n, s'en sert comme adresse pour obtenir la clé K correspondante et, à un instant précis, comme on le verra dans la suite, il l'applique en série au fil 25 vers le registre de chargement 12 de l'embrouilleur 1, Fig. 3.

Le compteur 44 est un diviseur-par-48 dont l'entrée de signal est reliée par un fil 48 relié à la sortie SYNC T du séparateur 13. La sortie du compteur 17, Fig. 3, est également reliée au microproces-

seur 42, par un fil 49, à chaque ligne 310 d'une trame. Le compteur 44 a encore une entrée de remise à zéro et une sortie respectivement reliées au microprocesseur 42 par des fils 50 et 51. Le fil 51 fournit la fréquence FT/48.

Un fil 52 relie le microprocesseur 42 et le circuit de gestion 31. En fonctionnement, le circuit de gestion 31, qui comporte un microprocesseur, est géré par un programme autonome qui, à intervalles prédéterminés, lui fait délivrer un nouvel article de contrôle d'accès $M_i(n)$ vers le générateur 32. Celui-ci, dans des conditions que l'on verra en détail dans la suite, fait transmettre ce message par le multiplexeur 2. Par l'intermédiaire du câble 38, du démodulateur 40 et du démultiplexeur 41, le microprocesseur 42 en prend connaissance et fait calculer par la carte 43 une nouvelle clé K(n), comme indiqué ci-dessus. Quand le calcul a été effectué et que la clé a été mise en mémoire, le microprocesseur 42 active le fil 52, indiquant au circuit de gestion 31 que cette clé K(n) est prête. Le circuit de gestion 31 entre cette information en mémoire à une adresse correspondant à n.

Le circuit de gestion 31 a une sortie reliée par un fil 53 à une entrée du microprocesseur 42. Le fil 53 sert au circuit de gestion 31 quand il demande l'autorisation d'émettre une clé de validation V(n).

Une sortie du microprocesseur 42 est reliée, par un fil 54, au circuit de gestion 31. Quand la demande d'autorisation d'émettre la clé V(n) a été examinée par le microprocesseur 42 et que celui-ci a terminé l'exécution d'un certain nombre d'actions qui seront détaillées dans la suite, il donne son autorisation d'émettre par le fil 54.

Enfin, entre la sortie du compteur 44 de l'unité de contrôle 4 et le circuit de gestion, est encore prévu un fil 55. On rappelle que le compteur 44 émet un signal toutes les quarante-huit trames.

Le programme de fonctionnement du microprocesseur 42 est, en fonctionnement courant, c'est-à-dire entre deux changements de clés, établi de la manière suivante:

- A chaque quarante-huitième trame signalée par le compteur 44, la ligne 310 est mise au blanc par le fil 29 et le chargement du registre 12 est assuré à partir de la valeur de la clé en

cours d'utilisation, laquelle se trouve dans sa mémoire. Il s'agit d'un rafraîchissement de clé qui s'exécute en activant le fil 26.

- Le démultiplexeur 41 est commuté par 45 pour recevoir la voie DIDON transmettant les messages $M_i(n)$.

Quand le microprocesseur 42 a reçu du circuit 31 une demande d'autorisation d'émettre V(n), son programme, une fois d'autres tâches éventuelles remplies, devient le suivant:

- Dans une première phase, il fait supprimer les mises au blanc périodiques de la ligne 310 pendant, par exemple, six cycles de quarante-huit trames, ce qui a pour objet de prévenir les récepteurs qu'un changement de clé va intervenir.
- Dans une seconde phase, le microprocesseur 42, par le fil 54, autorise le circuit 31 à émettre et, par ailleurs, par le fil 46, commute le démultiplexeur 41 de manière que celui-ci transmette le signal V(n) à venir.
- Dans une troisième phase, le microprocesseur fait rétablir les mises au blanc périodiques de la ligne 310. Dans le temps, la seconde phase se déroule après la première remise au blanc.

A la réception du signal d'autorisation par 54, le programme du circuit de gestion 31 devient le suivant:

- Il fait détecter le prochain signal de quarante-huitième trame émis par 44 sur 55, lequel correspond au premier intervalle de suppression trame où la ligne 310 est remise au blanc. Puis il déclenche un décompteur dont la capacité est de quarante-sept.

Le circuit de gestion 31 fait, par 33, émettre V(n) quatre fois dans le cycle ainsi déterminé, c'est-à-dire quand le compte du décompteur prend successivement les valeurs "15", "10", "5" et "1". Il en résulte que l'unité de commande 4 et les récepteurs du système reçoivent quatre fois V(n) dans un cycle déterminé de quarante-huit trames, le signal de validation donnant le nombre n permettant d'aller lire la clé K(n) dans la mémoire du microprocesseur 42.

A la quarante-huitième trame de ce cycle déterminé, le microprocesseur 42 présente la valeur de la clé K(n) sur le fil 25 et active le fil 26. Le fil 26 activé commande respectivement les multiplexeurs

18 et 19 pour qu'ils laissent passer les signaux transmis par 27 et par 25. Il en résulte que la nouvelle clé est chargée dans le registre 12 au rythme de l'horloge du microprocesseur 42 transmise par 27 et le multiplexeur 18. Dès que la nouvelle clé a été chargée dans le registre 12, l'horloge est supprimée sur 27, mais le fil 26 reste activé.

Au début de la fenêtre de chargement de la Fig. 6d, toujours dans la quarante-huitième trame, le fil 26 est désactivé, si bien que le multiplexeur transmet alors le signal SYNC L à l'entrée du registre 12. Par ailleurs, le multiplexeur 19 sert alors à reboucler la sortie du registre 12 vers son entrée.

De plus, quand le fil 26 est au repos, la sortie de l'inverseur 23 est activée, si bien que le multiplexeur 20 laisse entrer dans le registre 11 le signal de sortie du registre 12. L'entrée d'horloge du registre 11 reçoit en permanence le signal SYNC L. Ainsi, le contenu du registre 12 passe dans le registre 11 pendant la fenêtre de chargement au rythme de la synchronisation ligne.

A la fin de la fenêtre de chargement, c'est-à-dire à la fin de la vingtième ligne, si elle comprend vingt lignes correspondant aux vingt étages des registres 11 et 12, le fil 26 est de nouveau activé, ce qui commute les multiplexeurs 18 et 20. D'une part, l'horloge est supprimée sur le registre 12 dont le contenu a fait un tour complet. D'autre part, le contenu du registre 11 commence sa rotation.

On comprend qu'il suffit ensuite d'activer le fil 26 pendant la fenêtre de chargement toutes les quarante-huit trames pour rafraîchir la clé en rechargeant le contenu de 12 dans 11.

Le programme du microprocesseur 42 est tel qu'une fois le quatrième message V(n) reçu, il commute le démultiplexeur 41 en service, de manière à pouvoir à nouveau recevoir des messages $M_i(n)$. Le programme interne du circuit de gestion 31 est tel qu'il revient à l'état initial de commande d'émission des messages $M_i(n)$ par 32.

La Fig. 7a montre les périodes de quarante-huit trames symbolisées par des impulsions fournies par le compteur 44. La Fig. 7b illustre les positions temporelles des messages $M_i(n)$ émis par le circuit 32 du générateur de message 3. Il apparaît que les messages $M_i(n)$ sont groupés par trois. Dans chaque groupe, le même message est répété trois fois. Ces messages sont diffusés sur une voie DIDON,

reçus par le démodulateur DIDON de chaque récepteur, puis transmis au microprocesseur du récepteur qui se sert des trois messages pour éventuellement détecter et/ou corriger le message reçu. Leur position temporelle n'a pas besoin d'être rigidement liée aux cycles de quarante-huit trames de la Fig. 7a. Les groupes sont émis périodiquement, la période étant de l'ordre de 6 secondes. D'un groupe à un autre, la variable n peut changer.

La Fig. 8c illustre la fonction de la ligne 310 mise au blanc à chaque cycle de la Fig. 7a, tant qu'aucun message de validation V(n) n'est en cours de préparation de transmission. La Fig. 7d illustre la préparation d'une transmission de message V(n) avec suppression de lignes 310 au blanc, puis la transmission de V(n) dans le cycle qui suit le retour d'une ligne 310 au blanc. Il apparaît que le message V(n) est transmis quatre fois dans ce cycle. La transmission de V(n) est rigidement liée aux cycles.

Les Figs. 8a à 8c illustrent plus en détail les positions temporelles des messages V(n) dans leur cycle de transmission. La Fig. 8a montre les quarante-huit trames du cycle. La Fig. 8b montre les positions temporelles des lignes 310 au blanc. La Fig. 8c illustre le décompte effectué dans le décompteur du circuit 31, avec, en légende, les opérations effectuées.

La partie réception de la Fig. 2 comprend deux blocs: un désembrouilleur 7 et une unité de commande 8. La structure du désembrouilleur 7 est, comme généralement dans tous les systèmes d'embrouillage, semblable à celle de l'embrouilleur 1. Il comprend, Fig. 9, un générateur de séquence pseudo-aléatoire 56, un registre de chargement 57, un séparateur de synchronisations ligne et trame 58, un convertisseur analogique-numérique 59, un circuit de traitement 60, un multiplexeur 61 et un convertisseur numérique-analogique 62 qui délivre le signal vidéo désembrouillé.

Le désembrouilleur 7 comprend encore des circuits 63, 64, 65, 66 et 67 qui correspondent respectivement aux circuits 17, 18, 19, 20 et 23 de la Fig. 3. De plus, il comprend un circuit de détection de ligne au niveau du blanc 68 dont l'entrée est reliée à la sortie du convertisseur 59 et dont la sortie est reliée à une entrée d'une porte ET 69 dont la seconde entrée est reliée à la sortie du compteur 63. La sortie de la porte ET 69 est reliée à l'unité de commande 8

par une liaison 70. En pratique, la porte ET 69 sert à indiquer à l'unité 8 un trou dans la suite de lignes 310 mises au blanc, ce qui déclenche dans l'unité de commande 8 une commutation lui permettant de se mettre en attente des messages V(n).

Le signal vidéo embrouillé est appliqué aux circuits 58 et 59 par la liaison 71. Entre l'unité de commande 8 et le désembrouilleur 7, les liaisons 72, 73, 74, 75 et 76 correspondent respectivement aux liaisons 25, 26, 27, 48 et 49 de la Fig. 3 et jouent les mêmes rôles.

L'unité de commande 8 comprend un démodulateur DIDON 77, un démultiplexeur DIDON 78, un microprocesseur 79, un compteur 80 et elle peut recevoir une carte d'accès 81. A la Fig. 2, ces circuits sont représentés par de simples blocs car ils sont reliés entre eux comme les circuits correspondants de l'unité de commande de la Fig. 4. L'unité de commande 8 comprend encore une entrée 82 reliant le fil 70 au microprocesseur 79.

Le programme de fonctionnement du microprocesseur 79 est, en fonctionnement courant, c'est-à-dire entre deux changements de clés, établi de la manière suivante:

- A chaque ligne 310 reconnue mise au blanc, l'entrée 82 provoque une interruption du programme avec, pour résultat, le chargement du registre 56 pendant la fenêtre de chargement.
- le démultiplexeur 78 est commuté pour recevoir les messages $M_i(n)$ et les transmettre au microprocesseur 79.

Quand le programme de surveillance du microprocesseur 79 détecte une suite d'absences de signaux à l'entrée 82, le programme commute le multiplexeur 78 pour qu'il soit prêt à recevoir les messages V(n).

A la première réapparition de la ligne 310 au blanc, le signal à l'entrée 82 déclenche une surveillance de la réception des quatre messages V(n) attendus, comme on l'a défini plus haut. Il en résulte, dans la dernière trame du cycle, un nouveau chargement du registre 57, Fig. 9; puis le retour au programme antérieur. A titre indicatif, la réception des messages V(n) aux trames -15, -10, -5 et -1 permet au microprocesseur de s'assurer de la bonne marche de son compteur.

En outre, le programme du microprocesseur 79 accomplit d'autres tâches, telles que les communications avec la carte 81 pour le calcul de nouvelles clés K(n) à chaque réception de message $M_i(n)$, puis la

mise en mémoire de chaque clé à l'adresse n correspondante de sa mémoire.

A noter encore, que le chargement du registre 57 commence 2 ms après le signal de synchronisation trame, Fig. 6c, la durée de l'échange étant inférieur à 16 ms. Cette précaution est nécessaire car les 2 ms qui suivent la synchronisation trame sont utilisées pour le chargement du générateur de séquence pseudo-aléatoire 56 à partir du registre 57. Une fois le registre 57 chargé, le générateur 56 est initialisé et, au signal de synchronisation trame suivant, son chargement est effectué.

REVENDICATIONS

1) Système de télévision à contrôle d'accès utilisant une clé électronique variable (K(n)) permettant d'embrouiller l'information à l'émission et de la désembrouiller à la réception, la transmission de la clé (K(n)) de l'émetteur aux récepteurs étant effectuée d'une manière connue quelconque, caractérisé en ce qu'en plus de la clé, un signal de validation (V(n)) de clé est transmis de l'émetteur aux récepteurs.

2) Système suivant la revendication 1 caractérisé en ce que les différentes clés $M_i(n)$ contiennent une information n qui identifie leurs rangs, chaque signal de validation (V(n)) contenant également l'information n permettant d'identifier la clé (K(n)) à utiliser.

3) Système suivant la revendication 2, dans lequel chaque clé (K(n) est déterminée, dans chaque récepteur, à partir d'un message ($M_i(n)$) transmis par l'émetteur et une clé d'abonnement (C_i), caractérisé en ce que chaque message ($M_i(n)$) est répété plusieurs fois successivement à intervalles réguliers.

4) Système suivant la revendication 2 ou 3, caractérisé en ce que chaque signal de validation V(n) est transmis plusieurs fois dans des trames prédéterminées et à des intervalles de temps prédéterminés avant chaque validation de clé, la dernière transmission étant effectuée dans la trame qui précède le changement effectif de clé.

5) Système suivant l'une des revendications 1 à 4, caractérisé en ce que toutes les x trames (avec x égal à 48 par exemple) est transmis un signal de synchronisation de cycle de x trames (FT/48) qui provoque le chargement de la clé déjà validée.

6) Système suivant l'une des revendications 1 à 5, caractérisé en ce qu'un nombre prédéterminé de signaux successifs de synchronisation de cycle de x trames (FT/48) est supprimé avant chaque transmission de signal de validation V(n), le premier signal de synchronisation de cycle de x trames (FT/48)réapparaissant indiquant que le signal de validation ou la série de signaux de validation V(n) va être transmis dans le groupe de x trames suivant.

2583946

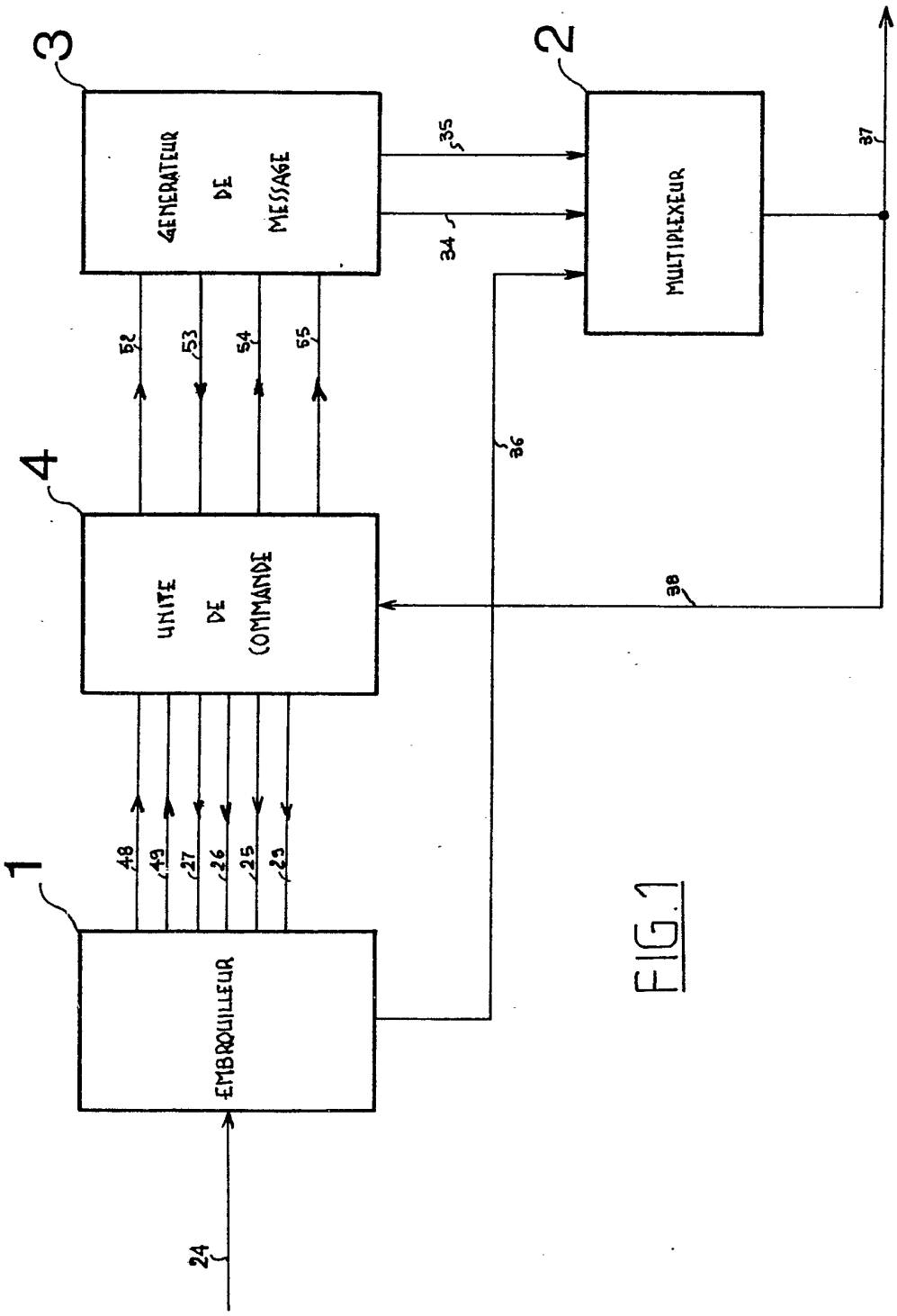


FIG. 1

2583946

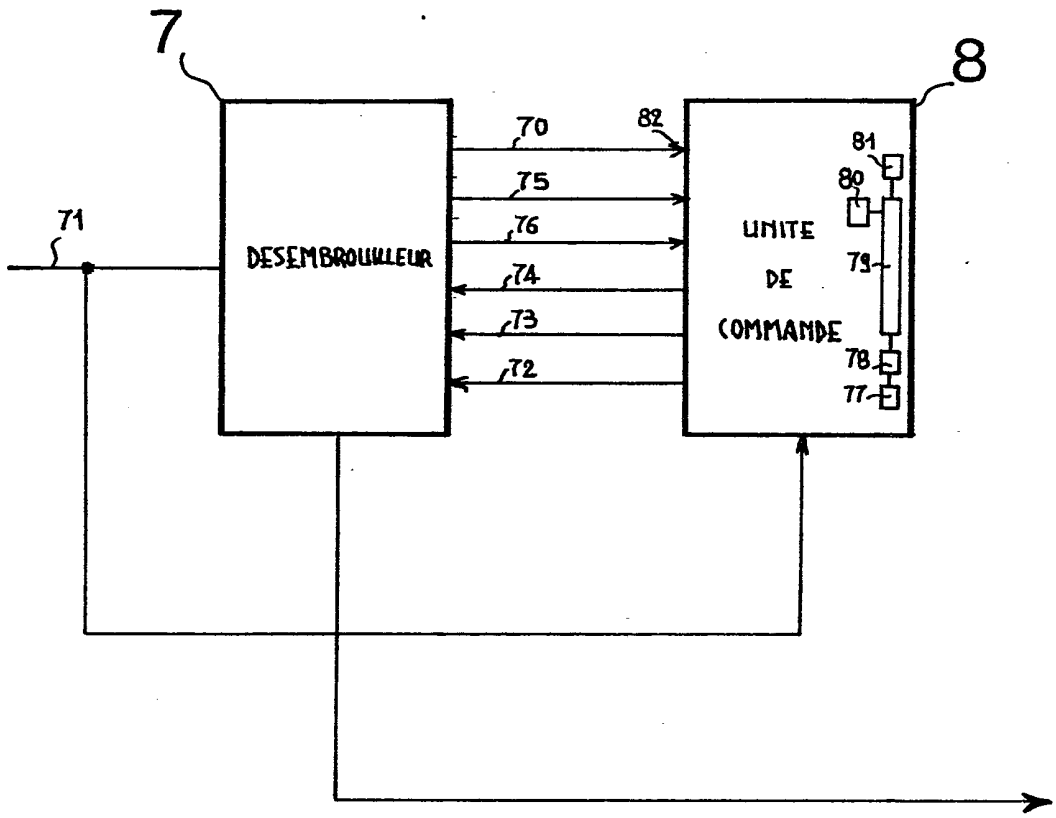


FIG. 2

2583946

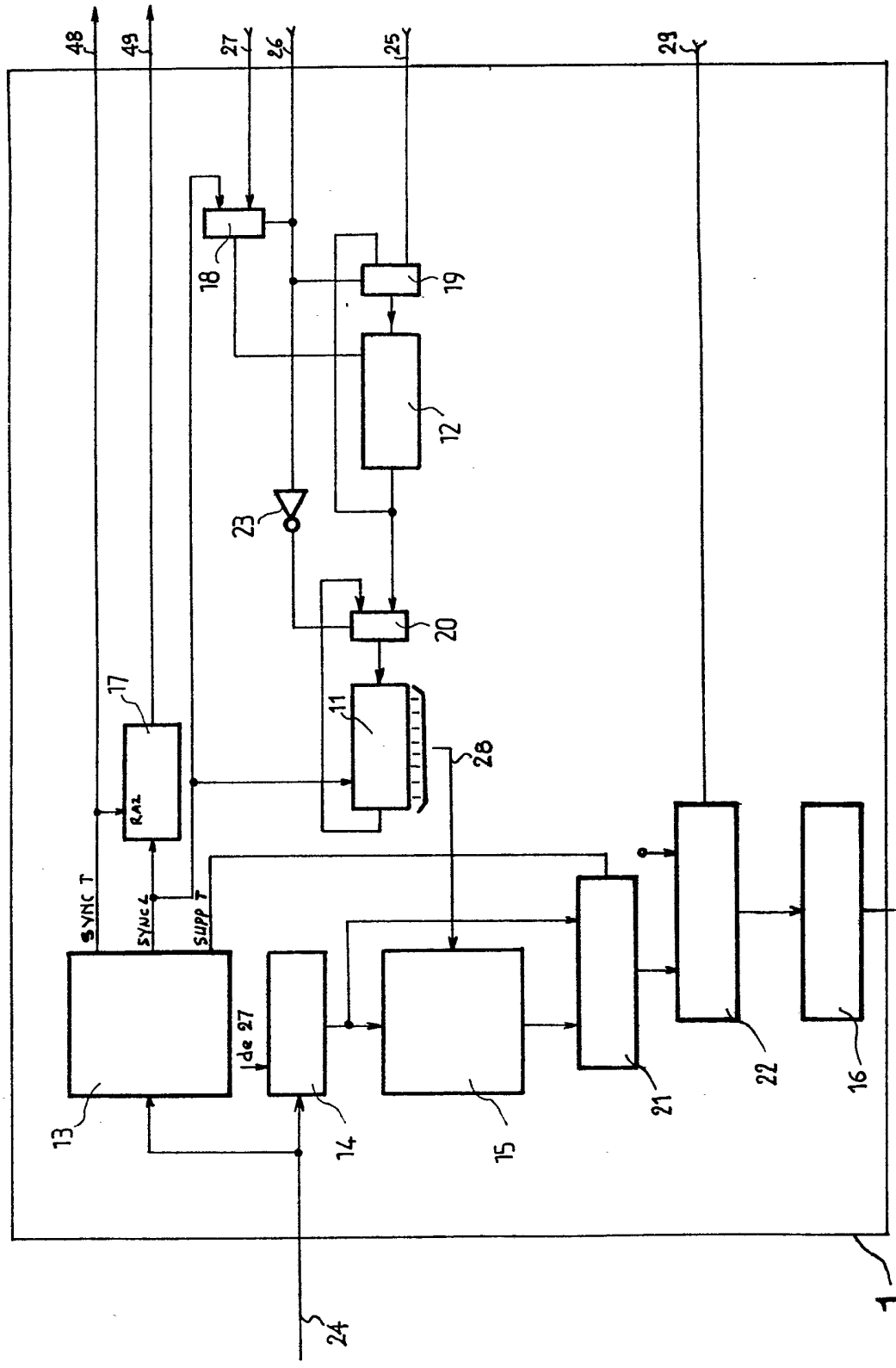
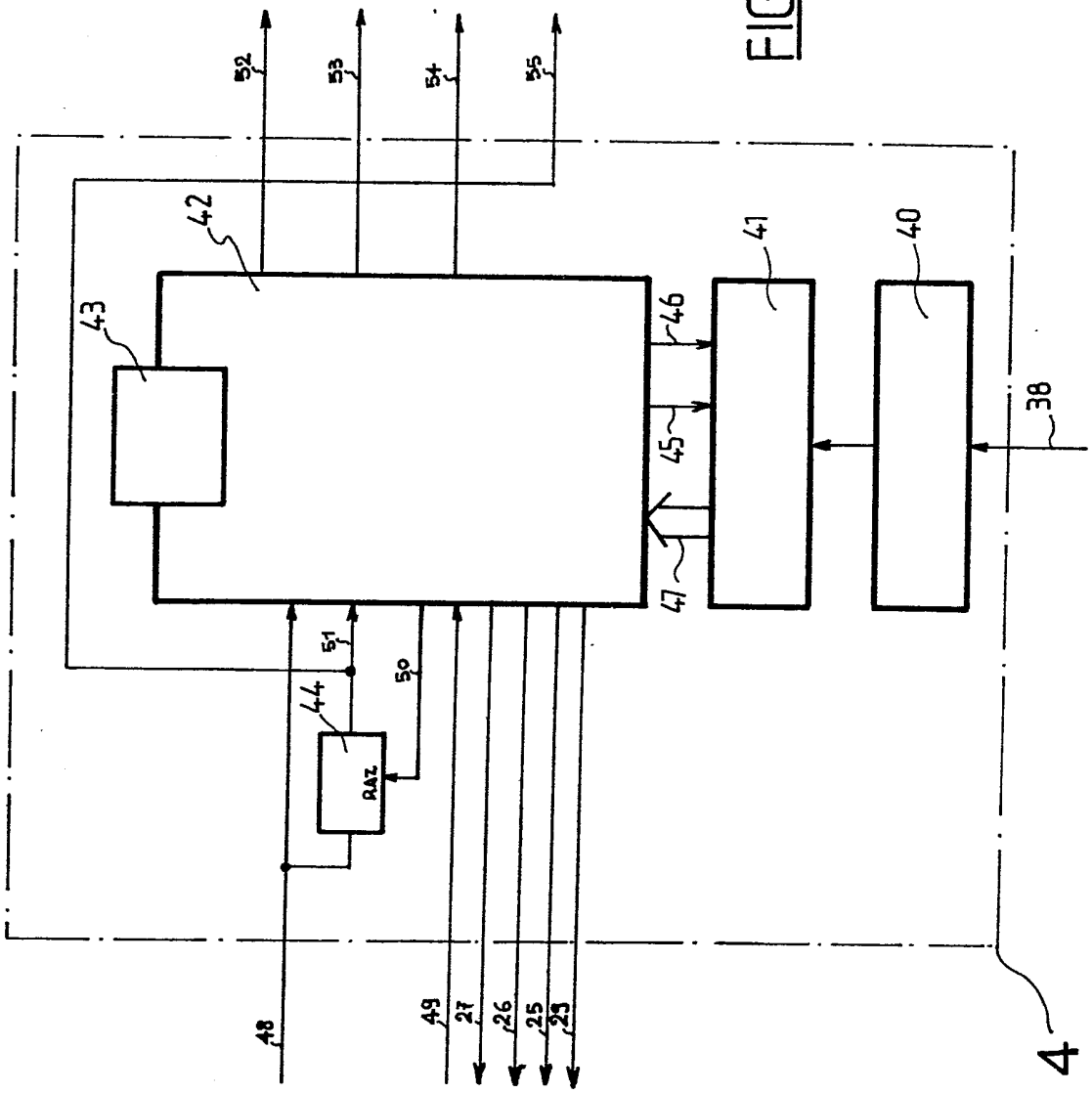


FIG.3

2583946

FIG.4



2583946

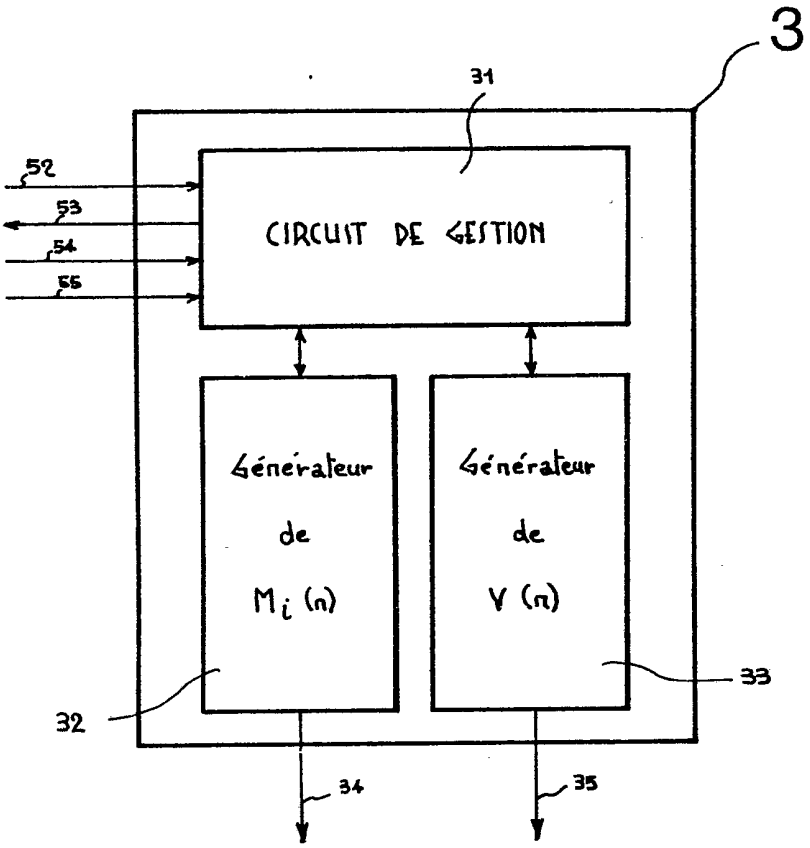
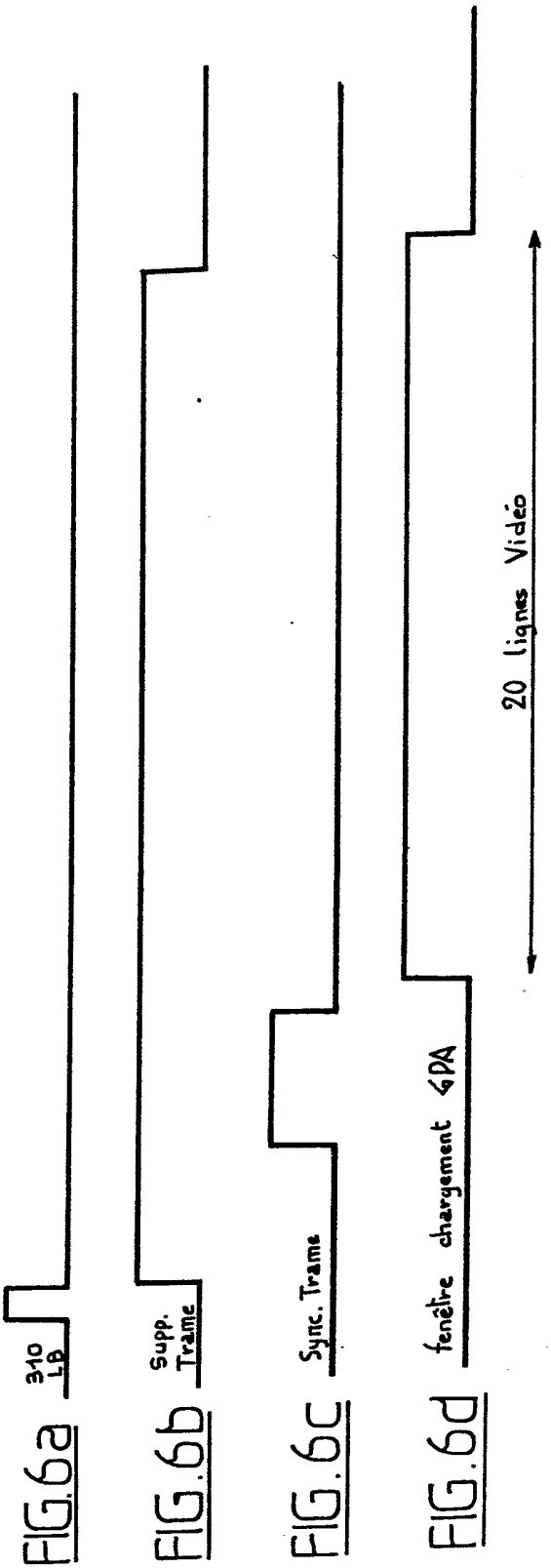
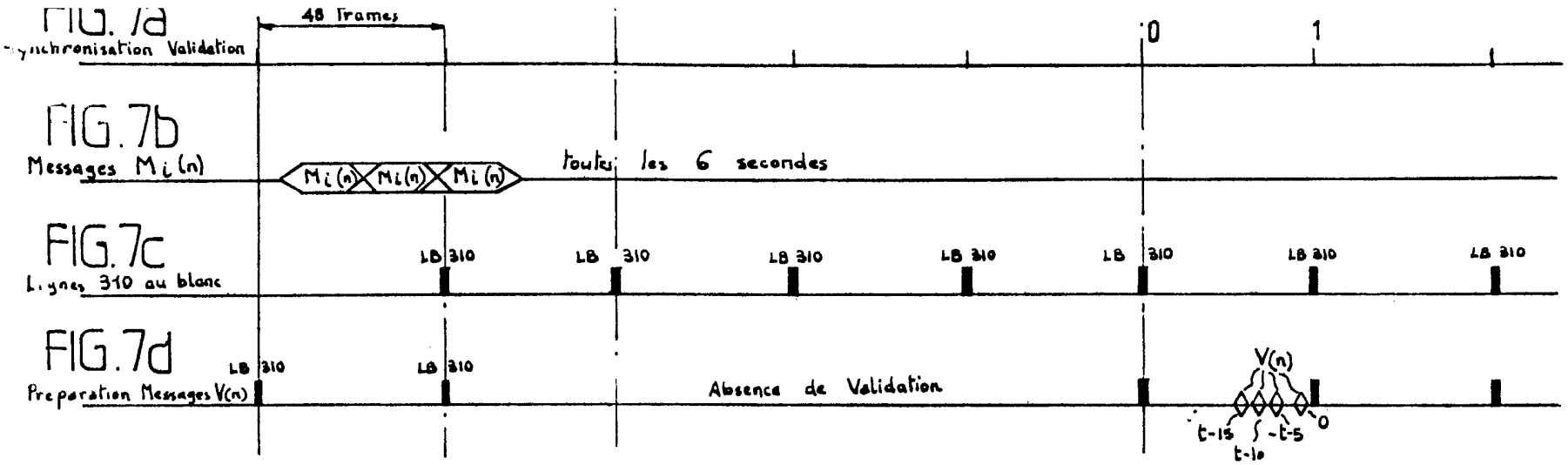
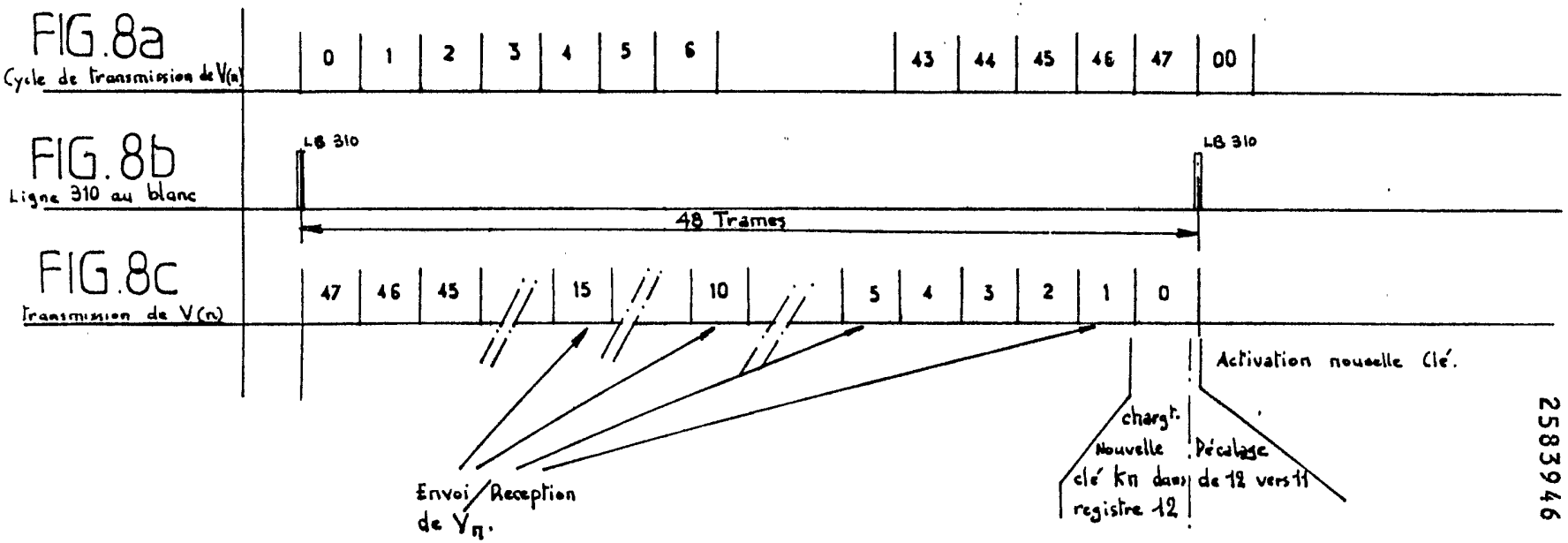


FIG.5

2583946


FIG.6a
310 LB
FIG.6b
Supp. Trame
FIG.6c
Sync. Trame
FIG.6d
fenêtre chargement 4PA
20 lignes Vidéo





PL. 7/8

2583946

2583946

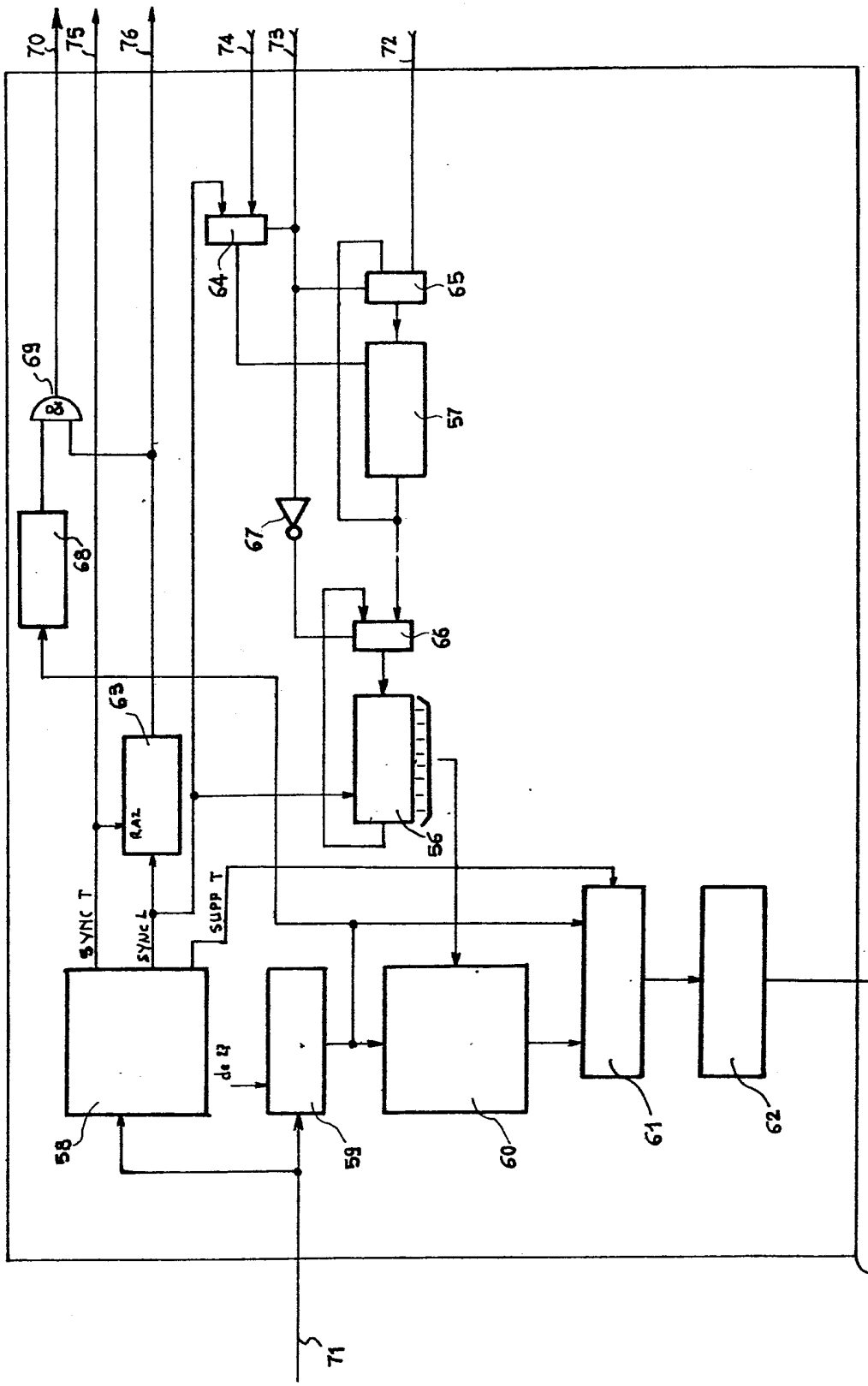


FIG.9