

Brevet N° **86240**
 du 8 janvier 1986
 Titre délivré : **9 JUNI 1986**

GRAND-DUCHÉ DE LUXEMBOURG



Monsieur le Ministre
 de l'Économie et des Classes Moyennes
 Service de la Propriété Intellectuelle
 LUXEMBOURG

Demande de Brevet d'Invention

I. Requête

La société dite: TECHNICAL DEVELOPMENTS & INVESTMENTS, (1)
 9492 ESCHEN, Liechtenstein, représentée par Monsieur
 Jacques de Muyser, agissant en qualité de mandataire (2)

dépose(nt) ce huit janvier 1900 quatre-vingt six (3)
 à 15 heures, au Ministère de l'Économie et des Classes Moyennes, à Luxembourg :
 1. la présente requête pour l'obtention d'un brevet d'invention concernant :
 "Procédés et dispositifs d'analyse et de reconnaissance du (4)
 code de cryptage d'émissions de télévision." (5)

2. la délégation de pouvoir, datée de Lausanne le 23 décembre 1985
 3. la description en langue française de l'invention en deux exemplaires;
 4. 5 planches de dessin, en deux exemplaires;
 5. la quittance des taxes versées au Bureau de l'Enregistrement à Luxembourg,
 le 8 janvier 1986

déclare(nt) en assumant la responsabilité de cette déclaration, que l'(es) inventeur(s) est (sont) :
 - François J. ZBERG, La Buselière, CH-1634 PONT-LA-VILLE, (5)
 Suisse

revendique(nt) pour la susdite demande de brevet la priorité d'une (des) demande(s) de
 (6) brevets déposée(s) en (7) Suisse
 le 9 janvier 1985 (No. 87/85) et le 22 mars 1985 (1289/85) (8)

au nom de la déposante (9)

élit(élisent) pour lui (elle) et, si désigné, pour son mandataire, à Luxembourg
 35, boulevard Royal (10)

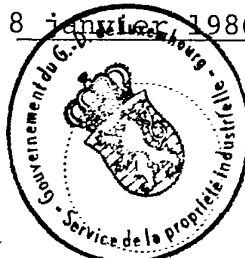
solicite(nt) la délivrance d'un brevet d'invention pour l'objet décrit et représenté dans les
 annexes susmentionnées, — avec ajournement de cette délivrance à // mois. (11)
 Le mandataire

II. Procès-verbal de Dépôt

La susdite demande de brevet d'invention a été déposée au Ministère de l'Économie et des
 Classes Moyennes, Service de la Propriété Intellectuelle à Luxembourg, en date du :

8 janvier 1986

à 15 heures



Pr. le Ministre
 de l'Économie et des Classes Moyennes,
 p. d.

REVENDEICATION DE LA PRIORITE

de la demande de brevet / ~~du modèle d'utilité~~

En Suisse

Du 9 janvier 1985 et

du 22 mars 1985

Mémoire Descriptif

déposé à l'appui d'une demande de

BREVET D'INVENTION

au

Luxembourg

au nom de : TECHNICAL DEVELOPMENTS & INVESTMENTS

pour : "Procédés et dispositifs d'analyse et de reconnaissance
du code de cryptage d'émissions de télévision."

Procédés et dispositifs d'analyse et de reconnaissance du code de cryptage d'émissions de télévision

La présente invention a trait au domaine de la télévision dite cryptée et concerne plus précisément la recherche du code de cryptage, utilisé dans le cadre du cryptage d'image télévisée par application de retards entre le signal image de chaque ligne vidéo et l'impulsion de synchronisation de ligne, ces retards étant variables et établis d'une ligne à l'autre d'après un code pseudo-aléatoire. Un tel cryptage détruit la structure verticale de l'image, la rendant inintelligible, les lignes étant décalées les unes par rapport aux autres et, pour une même ligne, d'une trame à l'autre de même parité dans un même cycle. Seule une compensation de ces retards à la réception permet de rétablir la synchronisation des différents signaux d'image d'une ligne à l'autre, le code de compensation étant lui-même fonction du code pseudo-aléatoire des retards utilisé lors du cryptage.

De tels dispositifs de cryptage et de décryptage existent à l'heure actuelle en Europe dans le cadre de télévisions à prépaiement, destinées à n'être décodées que par une certaine catégorie d'abonnés (cf. brevet français 75.34029 et demandes de brevets français 82.05006 et 82.05007).

Le but de l'invention est d'arriver à déterminer le cycle pseudo-aléatoire des décalages utilisé lors du codage, de manière à le restituer à un décodeur adapté qui sera alors capable de fournir une image correcte à partir de la version cryptée de l'image, ceci sans qu'il soit nécessaire à l'organisme crypteur de communiquer à chaque abonné le nouveau code de cryptage utilisé à chaque changement de celui-ci.

Il faut toutefois, pour que cette invention soit utilisable, que le code pseudo-aléatoire des décalages successifs entre le signal d'image vidéo de ligne et l'impulsion de synchronisation de cette même ligne, d'une ligne à l'autre, soit un code cyclique, c'est-à-dire établi pour

un nombre fini T de trames et réinitialisé au terme de ces T trames grâce à une indication de synchronisation de cycle portée par l'émission vidéo, l'émission audio ou les deux ensemble (par exemple, le cycle peut être réinitialisé toutes les 6 trames grâce à un niveau de blanc uniforme porté par la dernière ligne de la trame de fin de cycle, cette dernière ligne de trame restant noire, dans les 5 autres trames du cycle, comme le suggère la demande de brevet française No 82 05008).

Il faut en outre que le nombre des décalages différents possibles soit un nombre fini; appelons-le d (par exemple $d=3$, c'est-à-dire 3 types de décalages différents T_1 , T_2 , T_3 avec, par exemple, $T_1=0$, $T_2=s$, $T_3=2s$ et avec $s=1\mu s$).

Ces deux conditions sont effectivement réalisées dans le cadre des applications européennes actuelles de ce mode de cryptage.

L'invention dont il est question peut alors revêtir deux formes différentes:

- une forme dite pour l'analyse visuelle qui traite les signaux de manière à permettre à l'oeil humain de déterminer pour chacune des lignes du cycle de T trames la valeur du décalage, un dispositif permettant alors de mettre en mémoire pour chacune de ces lignes la valeur du décalage observé. La mémoire totale de toutes ces valeurs de décalages classées trame par trame et par lignes successives représentent alors le code pseudo-aléatoire recherché;
- une forme dite d'analyse automatique qui permet de remplacer l'oeil humain par un circuit électronique capable de juger, soit par un procédé comparatif, de la présence ou non d'un décalage entre 2 lignes successives d'une même trame, soit par un procédé d'analyse sur une plage donnée d'un palier de suppression.

Selon la première des deux formes ci-dessus, le procédé selon l'invention est défini par la revendication 1 et le dispositif pour le mettre en oeuvre par la revendication 10. Selon la seconde des deux formes ci-dessus, un

premier procédé automatique selon l'invention est défini par la revendication 6, un second procédé par la revendication 9 et les dispositifs pour les mettre en oeuvre par les revendications 14 respectivement 17.

Nous appellerons, dans le cadre de ce brevet et conformément aux spécificités techniques couramment en vigueur, "palier de suppression" la partie de la ligne vidéo débutant à la fin du front montant du top de synchronisation de ligne et terminant au début du signal image de cette même ligne vidéo supposée non cryptée ou correctement décryptée.

Un tel palier de suppression ne contient par conséquent aucune information d'image et sert à la référence de noir. Lorsqu'il sera question de "palier de suppression" pour une ligne vidéo cryptée, nous ferons référence à une partie de cette ligne vidéo débutant à la fin du front montant du top de synchronisation de ligne et de durée identique au palier de suppression d'une ligne vidéo non cryptée ou correctement décryptée.

Le second procédé d'analyse et de reconnaissance automatique du code de cryptage d'émissions de télévision consiste alors à essayer sur l'image vidéo cryptée successivement chacun des différents codes de cryptage possibles à l'aide d'un décodeur adapté et, pour un code donné, à rechercher sur un nombre déterminée de trames, grâce à un dispositif d'analyse portant sur certaines des lignes ainsi obtenues, la présence d'un signal image sur une plage d'analyse déterminée du palier de suppression de ces lignes, un tel signal étant significatif sur la ligne considérée de l'application d'un mauvais décryptage par le décodeur adapté.

Ainsi la présence d'un tel signal image sur la plage d'analyse déterminée du palier de suppression pour une seule des lignes examinées et pour le code considéré permet-il de rejeter ce code comme étant faux et de passer à l'analyse du code suivant.

Un tel procédé est notamment utilisable lorsque le nombre des codes pseudo-aléatoires différents possibles est faible, et qu'il existe entre chacun de ces différents codes des différences notables, ce qui est en particulier réalisé lorsque ces codes sont eux-mêmes issus d'un générateur pseudo-aléatoire capable de générer la séquence du code de cryptage pour un cycle complet à partir d'une clef de départ relativement courte. (De tels générateurs de codes pseudo-aléatoires sont utilisés à l'heure actuelle en Europe dans le cadre d'émissions télévisées cryptées par institution de retards, variables d'une ligne à l'autre, entre le signal image de la ligne vidéo et l'impulsion de synchronisation de ligne.)

De tels générateurs pseudo-aléatoires utilisent différents procédés logiques qu'il suffit de recréer, l'analyse ne nécessitant plus alors que de tester successivement chacune des différentes clefs de départ possibles (par exemple, si la clef de départ s'exprime sous la forme d'un mot de 11 bits, il y a 2^{11} , soit 2048 clefs différentes possibles qu'il suffit de tester une à une. Si chacun des tests nécessite 1 trame d'analyse, il faudra au maximum 41 secondes pour repérer la bonne clef et par conséquent connaître le code de cryptage utilisé, ce qui est relativement court).

Pour mieux comprendre l'invention, des formes d'exécution de l'invention vont être décrites en détail en se référant aux figures dans lesquelles

la figure 1 représente un dispositif d'analyse et de reconnaissance du code de cryptage mettant en oeuvre le procédé pour l'analyse visuelle,

la figure 2 représente un signal permettant de générer un index sur une ligne,

la figure 3 représente un dispositif d'analyse et de reconnaissance automatique du code de cryptage mettant en oeuvre un premier procédé d'analyse automatique,

la figure 4 représente le résultat d'une soustraction des signaux de deux lignes voisines d'une trame correcte ou décryptée et de deux lignes voisines cryptées ou

mal décryptées, selon le premier procédé d'analyse automatique,

la figure 5 représente un dispositif d'analyse et de reconnaissance automatique du code de cryptage mettant en oeuvre un second procédé d'analyse automatique et

la figure 6 représente différentes lignes vidéo dans le cadre du second procédé automatique.

Le procédé pour l'analyse visuelle consiste à analyser successivement chacune des T trames du cycle du code pseudo-aléatoire et, pour chacune de ces trames, successivement chacune des lignes la constituant, de manière à repérer pour chacune de ces lignes le décalage qui existe et l'enregistrer sur une mémoire à un emplacement lui correspondant dans le cycle. Une fois cette opération d'analyse réalisée pour toutes les lignes des T trames du cycle, la totalité des valeurs de décalage enregistrées, et classées par ordre de trame et de ligne, représente le code de cryptage recherché.

La figure 1 représente une vue très schématique d'un dispositif selon l'invention, mettant en oeuvre un procédé selon l'invention.

Ce dispositif comprend:

- a) Un extracteur de synchronisation 1 qui permet d'extraire les impulsions de synchronisation de ligne en 2 et de trame en 3 de l'image vidéo cryptée 100.
- b) Un extracteur de synchronisation de cycle de codage 4 lui-même fonction du type d'information vidéo de synchronisation de cycle prévue par l'organisme crypteur (dans l'exemple décrit, une information vidéo portée par la dernière ligne de la dernière trame de cycle) et capable de fournir des impulsions de synchronisation de cycle.
- c) Un commutateur vidéo (porte analogique) 5 qui permet de ne faire apparaître à l'écran 200 que celle des T trames du cycle en cours d'analyse, effaçant pour cela les lignes des T-1 autres trames du cycle et les remplaçant par un niveau de gris uniforme grâce au dispositif prévu en 7. Un tel

commutateur vidéo permet en outre de supprimer les décalages observés sur une même ligne d'une trame à l'autre de même parité, d'un même cycle et, chacune des lignes visualisées à l'écran restant ainsi à décalage fixe, permet à l'oeil humain une analyse précise du décalage absolu de chacune des lignes de la trame sélectionnée. Le gris uniforme permet quant à lui d'éviter une trop brusque variation de luminance entre deux trames sélectionnées à l'écran, par perte des T-1 trames intermédiaires, qui risquerait de fatiguer l'oeil excessivement compte tenu du phénomène de scintillement périodique toutes les T trames qui en résulterait. Le commutateur vidéo ainsi proposé est directement commandé par un circuit de sélection de trame 9.

d) Un circuit de sélection de trame 9 qui, d'une part, permet, grâce aux impulsions de synchronisation 2 et 3, de basculer le commutateur vidéo 5 en début de chaque ligne vidéo et de chaque trame, de manière à laisser passer l'information de synchronisation de ligne ou de trame et qui, d'autre part, permet, grâce à l'information de trame du cycle à sélectionner, issue du circuit compteur 50, d'une part de basculer le commutateur vidéo 5 sur toute la longueur de la trame sélectionnée et, d'autre part, de fournir au circuit de sélection de ligne 11 les impulsions de synchronisation de ligne des lignes de cette trame.

e) Un circuit de marquage de la ligne en cours d'analyse par affichage à l'écran en superposition sur une partie de cette ligne d'un index rectangulaire blanc. Un tel circuit est constitué d'un générateur d'index 15, dirigé par un pointeur d'index 13, qui n'est autre qu'un double monostable responsable, selon la figure 2, du positionnement de l'index à t_1 et pour une durée t_2 , sur la ligne en cours d'analyse. Ce pointeur d'index est lui-même commandé par un circuit de sélection de ligne 11.

f) Un circuit de sélection de ligne 11, qui permet de déclencher le pointeur d'index 13, et à travers lui le générateur d'index 15, au moment du passage de l'information vidéo correspondant à la ligne du cycle en cours d'analyse. Un tel circuit de sélection de ligne tient compte de l'in-

formation de ligne de trame à sélectionner provenant du circuit compteur 50 et reçoit du circuit de sélection de trame 9 les impulsions de synchronisation de ligne des lignes de la trame sélectionnée.

g) Un ensemble d'interrupteurs de validations 20 permettant la sélection manuelle des valeurs de décalage observées pour chacune des lignes analysées, étant bien entendu qu'il y a autant d'interrupteurs, ou de combinaisons d'interrupteurs, que de décalages différents possibles. L'information est alors directement transmise à la mémoire 66 où elle est stockée à une adresse correspondant à la ligne de la trame du cycle à laquelle elle se réfère, et permet l'analyse de la ligne suivante du cycle par incrémentation du circuit compteur 50. Un interrupteur particulier 21 permet de lancer l'analyse, la mémoire 66 étant prête à conserver le décalage sélectionné à la place correspondant à la 1ère ligne de la 1ère trame du cycle par une remise à zéro du compteur, toutes les informations précédemment stockées étant soit simplement effacées, soit déplacées dans un autre registre de mémoire avant effacement du registre de travail. On peut enfin également prévoir 2 interrupteurs supplémentaires d'avance et de retour destinés à modifier, par une avance ou un retour du circuit compteur, la ligne du cycle à analyser.

h) Une mémoire 66 et un circuit compteur 50 gérant cette mémoire, permettant au fur et à mesure de l'analyse ligne par ligne, de stocker la valeur du décalage observé et de restituer éventuellement un décodeur adapté chacune des valeurs de décalage préalablement stockée, au moment du passage vidéo de la ligne du cycle lui correspondant. Le circuit compteur permet quant à lui également d'informer le circuit de sélection de trame 9 et le circuit de sélection de ligne 11 de la trame ou de la ligne du cycle en cours d'analyse. Ce circuit compteur reçoit les impulsions de synchronisation de trame 3, de ligne 2 et de cycle issue de 4, ainsi que les impulsions d'incrémentation, issues de 20, à chaque validation d'une nouvelle valeur au sélecteur.

Un procédé utilisant le dispositif décrit permet donc, en fin d'analyse, d'aboutir à la connaissance du cycle pseudo-aléatoire de cryptage utilisé à l'émission.

Un tel procédé n'offre bien entendu d'intérêt que si le code pseudo-aléatoire utilisé reste fixe pendant une durée de temps assez importante (par exemple de l'ordre du mois), compte tenu du temps relativement long qu'il faut consacrer au procédé pour obtenir le code pseudo-aléatoire recherché (par exemple si $t=6$ trames et qu'il faut 1 seconde pour analyser chaque ligne, il faudra en tout à peu près 31 minutes de travail avant d'obtenir le code entier).

Un tel procédé peut enfin être couplé en temps réel avec un décodeur adapté 30, de manière à faire apparaître à l'écran, au fur et à mesure de l'analyse d'une trame, la partie déjà analysée sous forme décryptée. Pour ce faire, un circuit 40 reconnaît la mise en service du décodeur adapté 30 et permet de basculer le commutateur 41 de manière à remplacer l'information vidéo cryptée 100 par l'information vidéo issue du décodeur adapté, cette dernière conservant le décalage des lignes du cycle non encore analysées, la mémoire restituant pour ces lignes une valeur de décalage maximale, issue de la remise à zéro de la mémoire, et correspondant à un retard de compensation nul pour le décodeur adapté. L'ensemble de l'invention et du décodeur adapté, couplé, pouvant être considéré comme un "jeu vidéo" qui consisterait à faire apparaître l'image décodée le plus rapidement possible.

Une version simplifiée de ces procédé et dispositif d'analyse et de reconnaissance du code de cryptage pour l'analyse visuelle peut également être mise en oeuvre lorsque, d'une part le nombre des différents codes pseudo-aléatoires possibles est un nombre fini (appelons le N) et que, d'autre part, 2 codes quelconques pris parmi les N différents codes pseudo-aléatoires possibles n'ont, en une position déterminée du cycle, jamais plus de n valeurs successives de décalage, communes pour ces 2 codes.

Il suffit alors de limiter l'analyse visuelle décrite selon l'invention à n lignes successives du cycle prises en cette position déterminée du cycle, plus une ligne adjacente à ces n lignes - soit à la première, soit à la dernière des n lignes -, le circuit compteur 50 permettant dans cette version simplifiée de limiter l'analyse visuelle à ces $n+1$ lignes du cycle et de commander le circuit de reconnaissance 55 comprenant un micro-processeur, à l'issue de cette analyse, pour déterminer en fonction des $n+1$ valeurs stockées dans la mémoire 66 lequel des N différents codes pseudo-aléatoires possibles a été utilisé au cryptage, par comparaison de ces $n+1$ valeurs de décalage résultant de l'analyse avec successivement chacune des N séries de $n+1$ valeurs de décalage dont il dispose en mémoire et correspondant à chacun des N différents codes pseudo-aléatoires possibles en cette position du cycle. Une fois ce code identifié, le circuit de reconnaissance fournit une information spécifique de ce code au générateur de codes pseudo-aléatoires 61 qui lui-même restituera au décodeur adapté 30 les valeurs de décalage selon ce code, chacune au moment du passage dans l'émission vidéo télévisée de la ligne du cycle lui correspondant, ceci grâce aux impulsions de synchronisation de lignes, de trame et de cycle qu'il reçoit. Le décodeur adapté 30 permet alors grâce à ces valeurs de décalage de décrypter convenablement l'émission télévisée issue de 100 et de fournir la version décryptée directement au téléviseur 200.

Le procédé d'analyse automatique nécessite, pour être efficace, que le nombre des différents codes pseudo-aléatoires possibles ne soit pas infini. .

Le procédé consiste dans ce cas à essayer successivement chacun des différents codes possibles à l'aide d'un décodeur adapté (cf. demande de brevet français 83 05 006) et, pour un code donné, à vérifier sur un nombre déterminé de trames, grâce à un dispositif d'analyse ligne à ligne décrit dans l'invention, la

présence ou l'absence de décalages sur l'image vidéo obtenue.

Dans le cas où un nombre significatif de décalages serait observé, le code serait rejeté et un autre code serait analysé; dans le cas contraire, le code serait retenu comme étant le bon.

Un tel procédé est notamment utilisable lorsque le nombre des codes pseudo-aléatoires différents possibles est faible, et qu'il existe entre chacun de ces différents codes des différences notables, ce qui est en particulier réalisé lorsque ces codes sont eux-mêmes issus d'un générateur pseudo-aléatoire capable de générer la séquence du code de cryptage pour un cycle complet à partir d'une clef de départ relativement courte. (De tels générateurs de codes pseudo-aléatoires sont utilisés à l'heure actuelle en Europe dans le cadre d'émissions télévisées cryptées par institution de retards, variables d'une ligne à l'autre, entre le signal image de la ligne vidéo et l'impulsion de synchronisation de ligne.)

De tels générateurs pseudo-aléatoires utilisent différents procédés logiques qu'il suffit de recréer, l'analyse ne nécessitant plus alors que de tester successivement chacune des différentes clefs de départ possibles (par exemple, si la clef de départ s'exprime sous la forme d'un mot de 11 bits, il y a 2^{11} , soit 2048 clefs différentes possibles qu'il suffit de tester une à une. Si chacun des tests nécessite 1 trame d'analyse, il faudra au maximum 41 secondes pour repérer la bonne clef et par conséquent connaître le code de cryptage utilisé, ce qui est relativement court).

La figure 3 représente une vue très schématique d'un dispositif selon l'invention, mettant en oeuvre le procédé d'analyse automatique.

Un tel dispositif comprend:

- a) Un extracteur de synchronisation 1 permettant d'obtenir à partir de l'image vidéo 100 les impulsions de synchronisation de ligne en 2 et de trame en 3.
- b) Un extracteur de synchronisation de cycle de codage 4, lui-même fonction du type d'information vidéo de synchroni-

sation de cycle prévu par l'organisme crypteur (dans l'exemple décrit, une information vidéo portée par la dernière ligne de la dernière trame de cycle) et capable de fournir des impulsions de synchronisation de cycle.

c) Un générateur de code 60 capable de créer ou de restituer la totalité des codes pseudo-aléatoires différents possibles. Un tel générateur reçoit les impulsions de synchronisation de ligne 2, de trame 3 et les impulsions de synchronisation de cycle issue de 4.

d) Un décodeur adapté 30 capable de restituer, en présence du bon code de cryptage de l'image vidéo issu du générateur 60, une image vidéo parfaitement décryptée. En période d'analyse, ce décodeur adapté 30 reçoit les codes à tester du générateur 60 et transmet à l'analyseur 300 l'image vidéo transformée selon le code de décryptage fonction du code de cryptage analysé.

e) Un interrupteur 70 permettant de remettre à zéro le générateur de codes et par conséquent de redébuter l'analyse entière.

f) Un analyseur d'image 300 caractérisé en ce qu'il comprend:

- Un filtre réjecteur de la sous-porteuse couleur 10.

Il s'agit d'un circuit "bouchon" à 4,286 MHz pour le SECAM; 4,43 MHz pour le PAL; 3,58 MHz pour le NTSC. Un tel filtre permet de filtrer la chrominance pour ne conserver que la luminance.

- Une ligne à retard de valeur de retard une période de ligne (64 μ s pour le PAL ou le SECAM, 63,5 μ s pour le NTSC) pouvant être

- . soit une ligne à transfert de charge commandée par un générateur d'horloge,

- . soit une ligne à retard acoustique équipée de ses modulateur et démodulateur.

Une telle ligne de retard est chargée de retarder chaque ligne vidéo de manière à la comparer avec la ligne vidéo suivante de la même trame. La ligne vidéo retardée passe donc en e1 et la ligne vidéo suivante non retardée avec laquelle elle est comparée en e2.

- Un soustracteur 16 chargé de soustraire ces 2 lignes vidéo successives d'une même trame passant respectivement en e_1 et e_2 pour ne conserver que la différence que l'on analyse.

Comme le montre la figure 4, le résultat de cette soustraction est voisin de zéro lorsqu'il n'y a pas de décalage et que l'information portée par ces 2 lignes est presque identique (cas de gauche), alors qu'au contraire, s'il y a un décalage de temps t_0 entre ces 2 lignes (cas de droite), la soustraction donnera pour chacun des détails verticaux portés par ces lignes des portions de lignes positives et négatives de durée t_0 , sur la résultante de cette soustraction.

- Un générateur de fenêtre 18 tenant compte des impulsions de synchronisation 2 et de trame 3, chargé de déclencher des commutateurs de fenêtres 14, 14' de manière à ne conserver du signal vidéo entrant qu'un certain nombre de lignes pour chaque trame et qu'une partie centrale pour chacune de ces lignes.

Le premier commutateur de fenêtre 14 déclenché par le générateur de fenêtre 18 est chargé de ne conserver qu'un certain nombre de lignes pour chaque trame et qu'une partie centrale de l'information vidéo issue du soustracteur 16, comme le montre la figure 4 selon les exemples A et B, pour ces lignes.

- (d-1) voies d'analyse sélective en fréquence, placées en parallèle, chacune étant spécifique d'un des (d-1) différents temps de décalage possibles (le décalage nul n'étant pas pris en considération).

Chacune de ces (d-1) voies se compose:

- . d'un filtre passe-bande 22 adapté à l'un des (d-1) temps de décalage possible et chargé de ne conserver du signal d'entrée que la partie spécifiquement liée à ce temps de décalage,

- d'un détecteur de double alternance 23 chargé de détecter la présence du signal,

- d'un détecteur de niveau à seuil avec intégrateur 24 capable d'intégrer les informations de décalage de niveau supérieur à ce seuil, et d'informer le circuit logique de décision 45 à chaque obtention du niveau d'intégration.

- Un compteur de transitions constitué:

- du second commutateur de fenêtre 14', déclenché par le même générateur de fenêtre 18 et permettant de ne considérer qu'un certain nombre de lignes pour chaque trame et qu'une partie centrale de l'information vidéo de chacune de ces lignes,

- d'un détecteur à seuil 51 permettant de ne garder du signal vidéo pris en compte que la partie située au-dessus de ce seuil,

- d'un filtre passe-bande 52 permettant de ne laisser passer que les détails fins (de transition rapide) de l'image,

- d'un compteur 53 permettant de n'informer le circuit logique de décision 45 de la valeur analytique de la ligne considérée qu'à obtention d'un nombre minimum de détails fins. Ce compteur est automatiquement remis à zéro à chaque nouvelle ligne grâce à l'impulsion de synchronisation de ligne 2.

- Un circuit logique de décision 45 qui tient compte, pour un nombre déterminé de trames analysées, du nombre de lignes jugées analytiquement convenables par le compteur de transition et du nombre de décalages dénombrés par les (d-1) voies d'analyse sélective sur l'ensemble de ces lignes pour informer, sous forme d'un mot de 2 bits, le générateur de code 60 du résultat de l'analyse sur ces trames.

L'information de reconnaissance du code comme étant le bon est transmise sous la forme: 01; l'information de reconnaissance du code comme étant faux est transmise sous la forme: 10; enfin l'information de réanalyse de ce même code sous la forme: 00.

Un tel dispositif permet en fin de compte et après un temps d'analyse variable, fonction du nombre de codes à analyser avant de trouver le bon et de la qualité analytique des images prises en compte (un minimum de détails fins étant nécessaire), de reconnaître le bon code de cryptage et par conséquent de le donner à un décodeur adapté pour décrypter les émissions télévisées ainsi cryptées.

Un tel procédé n'est donc valable qu'à partir du moment où le temps de recherche automatique du code de cryptage est court par rapport au temps pendant lequel ce

code est appliqué (par exemple pour un code de cryptage valable un mois et une analyse de l'ordre de 30 minutes). Toutefois, dans le cas où le code de cryptage serait rapidement changé mais toujours choisi au sein d'un nombre restreint n de différents codes (par exemple $n=8$) fixés pour une durée de temps relativement longue (par exemple de l'ordre du mois), et si une information particulière, spécifique de celui des n codes utilisé à un instant donné, est véhiculée par l'information vidéo, ou l'information audio, ou les deux à la fois avant ou à chaque changement de code, il demeure possible de procéder selon l'invention, à condition de tenir compte pour chaque trame analysée du code parmi les n possibles, en cours d'utilisation, et de poursuivre l'analyse selon n sous-niveaux d'analyses dont il serait possible de passer de l'un à l'autre quelconque tout en conservant en mémoire les opérations d'analyse déjà effectuées sur chacun de ces sous-niveaux, et ce jusqu'à obtention de la valeur des n codes. Il suffira alors de les restituer chacun, en fonction de l'information spécifiant celui des n codes utilisé, pendant le temps d'utilisation respectif, à un décodeur adapté, pour obtenir une image parfaitement décryptée de la version cryptée de départ.

Voyons maintenant le second procédé d'analyse et de reconnaissance automatique.

La figure 6 représente, du point de vue de la luminance, dans le cadre d'un exemple de cryptage à 3 temps de décalage ($0, T, 2T$), et pour un signal image schématique dont le début est d'emblée un niveau moyen de blanc, l'ensemble des différentes lignes vidéo pouvant être obtenues à l'aide du décodeur adapté appliqué à l'image vidéo cryptée, en présence du bon code de cryptage (E), ou d'un mauvais code de cryptage (G) par rapport à l'ensemble des différentes lignes vidéo pouvant être obtenues au cryptage (F). L'exemple (E) représente également les lignes vidéo telles qu'elles sont reçues en l'absence de cryptage, toujours du point de vue de la luminance. H représente le palier de suppression et P une plage du palier de suppression sur laquelle peut se faire l'analyse, toute plage d'analyse choisie sur le palier de suppression se devant de contenir une partie au moins de cette plage P pour être opérationnelle.

La figure 5 représente un dispositif d'analyse et de reconnaissance automatique du code de cryptage mettant en oeuvre le second procédé d'analyse automatique par étude d'une plage du palier de suppression.

Un tel dispositif comprend:

- a) Un extracteur de synchronisation 1 permettant d'obtenir à partir de l'image vidéo 100 les impulsions de synchronisation de ligne en 2 et de trame en 3.
- b) Un extracteur de synchronisation du cycle de codage 4, lui-même fonction du type d'information vidéo de synchronisation de cycle prévue par l'organisme crypteur (dans l'exemple décrit, une information vidéo portée par la dernière ligne de la dernière trame du cycle), et capable de fournir des impulsions de synchronisation de cycle.
- c) Un générateur de code 60 capable de créer ou de restituer la totalité des codes pseudo-aléatoires différents possibles. Un tel générateur reçoit les impulsions de synchronisation de ligne 2, de trame 3 et les impulsions de synchronisation de cycle issues de 4.
- d) Un décodeur adapté 30 capable de restituer, en présence du bon code de cryptage de l'image vidéo issu du générateur 60, une image vidéo parfaitement décryptée.

En période d'analyse, ce décodeur adapté 30 reçoit les codes à tester du générateur 60 et transmet à l'analyseur 300 l'image vidéo transformée selon le code de décryptage fonction du code de cryptage analysé. Le décodeur adapté reçoit les impulsions de synchronisation de ligne 2 issues de l'extracteur de synchronisation 1.

e) Un interrupteur 70 permettant de remettre à zéro le générateur de codes et par conséquent de redébuter l'analyse entière, et un écran vidéo 200 permettant de visualiser l'image d'après le décodage effectué.

f) Un analyseur d'image 300 caractérisé en ce qu'il comprend:

- Un filtre réjecteur de la sous-porteuse couleur 10. Il s'agit d'un circuit "bouchon" à 4,286 MHz pour le SECAM; 4,43 MHz pour le PAL; 3,58 MHz pour le NTSC. Un tel filtre permet de filtrer la chrominance pour ne conserver que la luminance.
- Un circuit d'alignement au noir 26 permettant de restituer la composante continue du signal.
- Un circuit comparateur 27 qui délivre un niveau logique 1 lorsque le niveau du signal vidéo est supérieur à un niveau de référence choisi R.
- Un générateur de fenêtre 18 permettant de ne prendre en compte dans l'analyse que certaines lignes pour chaque trame et, pour ces lignes, qu'une certaine plage du palier de suppression. Ce générateur de fenêtre délivre un niveau logique 1 à l'intérieur des temps pris en compte dans l'analyse.
- Une porte logique "ET" 28 qui traite les informations issues du générateur de fenêtre d'une part, et du circuit comparateur d'autre part.
- Un circuit de décision 29 qui, en fonction du nombre des impulsions reçues par trame, informe le générateur de code 60, sous forme d'un mot de 2 bits, du résultat de l'analyse sur cette trame. L'information de reconnaissance du code comme étant le bon est transmise sous la forme: 01; l'information de reconnaissance du code comme étant faux sous la forme: 10; enfin l'information de réanalyse de ce même code sous la forme: 00, tant qu'un nombre suffisant de trames n'a pas été pris en compte dans l'analyse du code.

Un tel dispositif permet en fin de compte et après un temps d'analyse variable, fonction du nombre de codes à analyser avant de trouver le bon et de la qualité analytique des lignes prises en compte (un minimum de luminance en tout début du signal image étant nécessaire), de reconnaître le bon code de cryptage et par conséquent de le donner à un décodeur adapté pour décrypter les émissions télévisées ainsi cryptées.

Un tel procédé n'est donc valable qu'à partir du moment où le temps de recherche automatique du code de cryptage est court par rapport au temps pendant lequel ce code est appliqué (par exemple pour un code de cryptage valable un mois et une analyse de l'ordre de 30 minutes). Toutefois, dans le cas où le code de cryptage serait rapidement changé mais toujours choisi au sein d'un nombre restreint n de différents codes (par exemple $n=8$) fixés pour une durée de temps relativement longue (par exemple de l'ordre du mois), et si une information particulière, spécifique de celui des n codes utilisé à un instant donné, est véhiculée par l'information vidéo, ou l'information audio, ou les deux à la fois avant ou à chaque changement de code, il demeure possible de procéder selon l'invention, à condition de tenir compte pour chaque trame analysée du code parmi les n possibles, en cours d'utilisation, et de poursuivre l'analyse selon n sous niveaux d'analyses dont il serait possible de passer de l'un à l'autre quelconque tout en conservant en mémoire les opérations d'analyse déjà effectuées sur chacun de ces sous-niveaux, et ce jusqu'à obtention de la valeur des n codes. Il suffira alors de les restituer chacun, en fonction de l'information spécifiant celui des n codes utilisé, pendant le temps d'utilisation respectif, à un décodeur adapté, pour obtenir une image parfaitement décryptée de la version cryptée de départ.

Les procédés et dispositifs selon l'invention peuvent être également utilisés pour la recherche du code de cryptage lorsque les émissions de télévision sont non seulement cryptées comme indiqué dans le préambule des revendications 1,6 et 9, mais

appliquent également un procédé d'inversion de polarité du signal vidéo (tel que décrit dans la demande de brevet français 75 34029), opéré sur une ou plusieurs lignes déterminées du cycle et pour chaque cycle sur les mêmes lignes. De telles inversions de polarité peuvent être reconnues soit par l'opérateur procédant à l'analyse visuelle soit par un circuit simple; le signal peut alors être restitué corrigé de cette inversion de polarité ce qui permet d'appliquer les procédés et dispositifs de la présente invention. L'information indiquant que telle ligne du cycle a subi une inversion de polarité peut facilement être conservée dans une mémoire complétant celle conservant les valeurs de décalage, et l'information être restituée au décodeur adapté de façon à rectifier cette inversion de polarité conjointement à la compensation des décalages qu'il opère.

Il faut également noter que, sans sortir du cadre de l'invention, il demeure possible de procéder selon l'invention avec moins de $d - 1$ voies d'analyse sélective en fréquence dès lors que l'on est sûr de détecter avec les voies d'analyses prises en compte et pour tous les différents codes possibles, sauf le bon, un nombre minimum de décalages par groupe de trames analysé.

Revendications

1. Procédé d'analyse et de reconnaissance du code de cryptage d'émissions de télévision pour l'analyse visuelle, le cryptage étant obtenu par imposition d'un retard, variable d'une ligne à l'autre, entre le signal image de la ligne vidéo et l'impulsion de synchronisation de ligne, ces retards étant établis d'une ligne à l'autre selon un code pseudo-aléatoire réinitialisé de manière cyclique toutes les T trames, caractérisé par un traitement du signal crypté consistant, pour chaque cycle, à ne faire apparaître sur un écran qu'une première trame des T trames du cycle en effaçant les T-1 autres trames du cycle, cette opération étant répétée pendant le temps nécessaire à l'analyse de toutes les lignes constituant cette trame du cycle, à conserver en mémoire une valeur de retard introduite à un sélecteur par un opérateur selon son estimation du décalage de la première ligne analysée, puis à conserver en mémoire à une seconde place la valeur sélectionnée par l'opérateur pour la seconde ligne et ainsi de suite pour toutes les lignes de la première trame, puis de la seconde trame et ainsi de suite jusqu'à la dernière trame du cycle, les valeurs de retard étant classées en mémoire par ordre de trame puis de ligne du cycle, constituant ainsi le code pseudo-aléatoire de cryptage cherché.

2. Procédé selon la revendication 1, caractérisé en ce qu'il permet de marquer à l'écran la ligne en cours d'analyse, grâce à la superposition sur une partie de cette ligne d'un index blanc.

3. Procédé selon la revendication 1 ou 2, caractérisé en ce qu'il permet de remplacer, au cours de l'analyse d'une des T trames du cycle, les T-1 autres trames du cycle qui sont effacées par autant de trames composées de lignes toutes identiques et correspondant à un niveau de gris uniforme, de manière à modérer le phénomène de scintillement toutes les T trames qui résulte de cet effacement.

4. Procédé selon l'une des revendications 1 à 3, caractérisé en ce que les valeurs de retard sélectionnées sont directement appliquées par un décodeur adapté à la

compensation pour chaque cycle des décalages de ligne auxquels elles se rapportent.

5. Procédé selon la revendication 1, caractérisé en ce que, lorsque le code pseudo-aléatoire utilisé est pris parmi un nombre fini de différents codes de cryptage pseudo-aléatoires possibles et qu'il n'existe, entre deux quelconques de ces différents codes possibles, jamais plus de n valeurs successives de décalage, communes pour ces deux codes, en une position déterminée du cycle, il suffit de limiter l'analyse visuelle à ces n lignes successives du cycle plus une ligne, adjacente à la première ou à la dernière de ces n lignes successives du cycle, un circuit de reconnaissance (55) permettant alors de déterminer, grâce aux $n + 1$ valeurs successives de décalage stockées à l'issue de l'analyse, celui des différents codes pseudo-aléatoires de cryptage utilisé.

6. Procédé d'analyse et de reconnaissance du code de cryptage d'émissions de télévision selon une méthode d'analyse automatique, le cryptage étant obtenu par imposition d'un retard, variable d'une ligne à l'autre, entre le signal image de la ligne vidéo et l'impulsion de synchronisation de ligne, ces retards étant établis d'une ligne à l'autre selon un code pseudo-aléatoire réinitialisé de manière cyclique toutes les T trames, caractérisé en ce qu'un premier code pseudo-aléatoire de cryptage possible est généré par un circuit adéquat, qu'un décodeur applique les valeurs de retard complémentaires, correspondant à ce premier code, au décryptage des lignes d'au moins une trame correspondante du cycle, qu'un circuit d'analyse contrôle sur chacune des trames ainsi obtenues la présence de décalages entre les lignes successives, prises deux à deux, de cette trame en retardant le signal de chaque ligne de la valeur d'une période de ligne et en le soustrayant de celui de la ligne suivante, pour repérer sur la différence la présence de signaux significatifs de décalage, que lorsque un nombre minimum de décalages de lignes est constaté après l'analyse de ces trames, un second code de cryptage est généré et l'opération d'analyse est répétée, puis un troisième code de cryptage, etc. jusqu'à ce que le code de

cryptage généré produise, grâce à ce décodeur, des trames pour l'ensemble desquelles moins d'un nombre déterminé de décalages est perçu entre les lignes successives de chacune d'entre elles, ce qui entraîne la fin de l'analyse et la mise en mémoire du dernier code employé.

7. Procédé selon la revendication 6, caractérisé en ce que le résultat de l'analyse du dernier code retenu n'est jugé valable que si les informations vidéo portées par les trames ayant permis l'analyse de ce code sont jugées favorables, ceci par la présence d'un minimum de "détails fins" dans l'image permettant au circuit d'analyse de travailler efficacement.

8. Procédé selon la revendication 6 ou 7, caractérisé en ce que lorsque le cryptage applique un retard pris parmi $d-1$ temps différents possibles et un retard nul, le circuit d'analyse opère avec au plus $d-1$ voies d'analyse sélective en fréquence, placées en parallèle, chacune étant spécifique d'un des $d-1$ différents temps de décalage possibles.

9. Procédé d'analyse et de reconnaissance automatique du code de cryptage d'émissions de télévision, le cryptage étant obtenu par imposition d'un retard, variable d'une ligne à l'autre, entre le signal image de la ligne vidéo et l'impulsion de synchronisation de ligne, ces retards étant établis d'une ligne à l'autre selon un code pseudo-aléatoire réinitialisé de manière cyclique toutes les T trames, caractérisé en ce qu'un premier code pseudo-aléatoire de cryptage possible est généré par un circuit adéquat, qu'un décodeur applique les valeurs de retard complémentaires, correspondant à ce premier code, au décryptage des lignes correspondantes du cycle, qu'un circuit d'analyse recherche sur certaines des lignes ainsi obtenues la présence d'un signal image sur une plage donnée du palier de suppression, en ce que lorsque dans un minimum de ces lignes pour un groupe de trames considéré, un signal image est perçu sur la plage donnée du palier de suppression, un second code de cryptage est généré et l'opération d'analyse est répétée, puis un troisième code de cryptage, etc. jus-

qu'à ce que le code de cryptage généré produise à l'aide du décodeur des lignes, dont celles prises en compte dans l'analyse, et pour un groupe déterminé de trames, qui ne débute pas leur signal image sur la plage du palier de suppression choisie pour l'analyse sauf exceptions, le nombre des exceptions étant inférieur à un nombre déterminé, ce qui entraîne la fin de l'analyse et la mise en mémoire du dernier code employé.

10. Dispositif pour la mise en oeuvre du procédé selon la revendication 1, caractérisé en ce qu'il comprend

a) un extracteur de synchronisation (1) qui permet d'extraire les impulsions de synchronisation de ligne (2) et de trame (3) du signal de télévision reçu crypté (100);

b) un circuit d'analyse des informations de synchronisation de cycle (4), qu'elles soient vidéo ou audio ou les deux, et permettant de générer des impulsions de synchronisation de cycle;

c) un sélecteur (20) auquel l'opérateur introduit la valeur de retard correspondant à son estimation de la valeur de décalage observée sur la ligne analysée;

d) une mémoire (66) capable de mémoriser chacune des valeurs de décalage sélectionnée par l'opérateur au sélecteur, à une adresse correspondante du cycle;

e) un circuit compteur (50) recevant les impulsions de synchronisation de ligne, de trame et de cycle ainsi que des impulsions d'incrémentation à chaque validation d'une nouvelle valeur de décalage au sélecteur, permettant, d'une part de gérer la mémoire et, d'autre part, d'informer le circuit de sélection de trame de la trame du cycle, portant la ligne en cours d'analyse, à sélectionner;

f) un circuit de sélection de trame (9) qui reçoit l'information de trame du cycle à sélectionner du circuit compteur, ainsi que les impulsions de synchronisation de ligne, de trame et de cycle, et un commutateur vidéo (5) commandé par le circuit de sélection de trame, ces deux circuits étant agencés de façon à oc-

culturer pour chacun des cycles de T trames et pour chaque valeur de trame à sélectionner les informations vidéo de ligne - mais non les informations de synchronisation de lignes ou de trame - portées par les T-1 trames différentes de celle du cycle qui est à sélectionner et qui, elle, est intégralement transmise.

11. Dispositif selon la revendication 10 pour la mise en oeuvre du procédé selon les revendications 2 et 3, caractérisé en ce qu'il comprend en plus des circuits générant un index (11, 13, 15) marquant la ligne en cours d'analyse, et recevant du circuit compteur l'information de ligne à sélectionner et du circuit de sélection de trame les impulsions de synchronisation de ligne sur toute la longueur de la trame sélectionnée, et un circuit générateur de niveau de gris uniforme (7) qui transmet à la place de chacune des informations vidéo de ligne des T-1 trames du cycle, qui sont occultées par le commutateur vidéo, un signal de niveau correspondant au gris uniforme.

12. Dispositif selon la revendication 10 ou 11, caractérisé en ce qu'il comprend en plus un décodeur adapté (30) couplé avec la mémoire (66) et qui décrypte chacune des lignes du cycle précédemment analysées en fonction des valeurs respectives de décalage stockées en mémoire et un circuit logique (40) associé avec un autre commutateur vidéo (41) pour afficher à l'écran les informations vidéo issues du décodeur adapté, les lignes étant ainsi décryptées lorsqu'une valeur de décalage a été mémorisée et non décryptées lorsque la valeur de décalage coïncide avec celle enregistrée à chaque remise à zéro de la mémoire et correspondant à un décalage maximal, le décodeur adapté opérant alors un décalage de compensation nul.

13. Dispositif selon l'une des revendications 10 à 12 pour la mise en oeuvre du procédé selon la revendication 5, caractérisé en ce que le circuit compteur (50) ne réalise l'analyse visuelle que sur n+1 lignes successives du cycle prises en une position déterminée du cycle, ^{et en ce qu'il comprend,} un circuit de reconnaissance (55) comprenant un microprocesseur commandé par le circuit compteur et capable, à l'issue de l'analyse visuelle, de comparer les

$n+1$ valeurs de décalage stockées dans la mémoire (66) avec chacune des séries de $n+1$ valeurs de décalage qu'il possède en mémoire et qui correspondent à chacun des différents codes pseudo-aléatoires possibles en cette position déterminée du cycle, et un générateur de codes pseudo-aléatoires (61) auquel il transmet une information spécifique du code qu'il a reconnu, ce générateur restituant alors le code de cryptage recherché.

14. Dispositif pour la mise en oeuvre du procédé selon la revendication 6, caractérisé en ce qu'il comprend

a) un extracteur de synchronisation (1) qui permet d'extraire les impulsions de synchronisation de ligne (2) et de trame (3) du signal de télévision reçu crypté (100);

b) un circuit d'analyse des informations de synchronisation de cycle (4), qu'elles soient vidéo ou audio ou les deux, et permettant de générer des impulsions de synchronisation de cycle;

c) un circuit générateur de codes (60), capable de créer ou de restituer successivement tous les différents codes de cryptage pseudo-aléatoires possibles et recevant les impulsions de synchronisation de ligne, de cycle et de trame;

d) un décodeur adapté (30) capable d'appliquer un retard de décryptage à chaque ligne, en fonction de la valeur du décalage de cryptage fournie par le générateur de code, pour un code donné, successivement pour chacune des lignes du cycle au moment de son passage respectif;

e) un circuit d'analyse d'image (300), auquel est transmis la version traitée par le décodeur, selon le code à analyser, de l'image vidéo cryptée de départ, comportant:

- un filtre réjecteur (10) de la sous-porteuse couleur, permettant de ne conserver de l'information vidéo que la luminance;
- une ligne de retard (12), de retard une période de ligne, chargée de retarder chaque ligne vidéo pour la comparer avec la ligne vidéo suivante de la même trame;
- un soustracteur (16) chargé de soustraire les informations vidéo des deux lignes successives obtenues précédemment,

pour ne conserver que la différence;

- au plus d-1 voies d'analyse sélective en fréquence, placées en parallèles, chacune étant spécifique d'un des d-1 différents temps de décalage possibles, le décalage nul n'étant pas pris en considération, chaque voie comportant un filtre passe-bande (22) adapté à l'un des d-1 temps de décalage possibles et un détecteur de niveau à seuil avec intégrateur (24);

- un circuit logique de décision (45) qui, en fonction du nombre des impulsions reçues des détecteurs à seuil avec intégrateurs (24), pour un nombre déterminé de trames, informe le générateur de code de ce que le code analysé est le bon ou non, cette dernière interprétation entraînant l'analyse d'un autre code de cryptage.

15. Dispositif selon la revendication 14 pour la mise en oeuvre du procédé selon la revendication 7, caractérisé en ce qu'il comprend en plus un compteur de transitions constitué:

- d'un détecteur à seuil (51),
- d'un filtre passe-bande (52),
- d'un compteur (53) pour déterminer si les informations vidéo contemporaines de l'analyse sont favorables et informer en conséquence le circuit logique de décision si le résultat donné par les voies d'analyse sélective en fréquence peut être validé ou non.

16. Dispositif selon la revendication 14 ou 15, caractérisé en ce qu'il comprend en plus:

- un générateur de fenêtre (18) recevant les impulsions de synchronisation de ligne et de trame chargé de basculer les commutateurs de fenêtres (14,14') de manière à ne conserver du signal vidéo d'entrée qu'un certain nombre de lignes pour chaque trame et qu'une partie centrale pour chacune de ces lignes;
- des commutateurs de fenêtre (14,14'), commandés par le générateur de fenêtre, l'un (14) étant appliqué au signal vidéo issu du soustracteur (16) du circuit d'analyse et/ou l'autre (14') étant appliqué au signal vidéo pris en compte par le compteur de transitions (51,52,53).

17. Dispositif pour la mise en oeuvre du procédé selon la revendication 9, caractérisé en ce qu'il comprend

- a) un extracteur de synchronisation (1) qui permet d'extraire les impulsions de synchronisation de ligne (2) et de trame (3) du signal de télévision reçu crypté (100);
- b) un circuit d'analyse des informations de synchronisation de cycle (4), qu'elles soient vidéo ou audio ou les deux, et permettant de générer des impulsions de synchronisation de cycle;
- c) un circuit générateur de codes (60), capable de créer ou de restituer successivement tous les différents codes de cryptage pseudo-aléatoires possibles et recevant les impulsions de synchronisation de ligne, de cycle et de trame;
- d) un décodeur adapté (30) capable d'appliquer un retard de décryptage à chaque ligne, en fonction de la valeur du décalage de cryptage fournie par le générateur de code, pour un code donné, successivement pour chacune des lignes du cycle au moment de son passage respectif;
- e) un circuit d'analyse d'image (300'), auquel est transmise la version traitée par le décodeur, selon le code à analyser, de l'image vidéo cryptée de départ, comportant:
 - un filtre réjecteur (10) de la sous-porteuse couleur, permettant de ne conserver de l'information vidéo que la luminance;
 - un circuit d'alignement au noir (26) permettant de restituer la composante continue du signal;
 - un circuit comparateur (27) qui délivre un niveau logique 1 lorsque le niveau du signal est supérieur à un niveau de référence choisi;
 - un générateur de fenêtre (18) permettant de ne prendre en compte dans l'analyse que certaines lignes pour chaque trame et, pour ces lignes, qu'une certaine plage du palier de suppression, ce générateur de fenêtre délivrant un niveau logique 1 à l'intérieur des intervalles de temps pris en compte dans l'analyse;
 - une porte logique "ET" (28) qui traite les informations issues du générateur de fenêtre d'une part, et du circuit comparateur d'autre part;

- un circuit de décision (29) qui, en fonction du nombre des impulsions reçues par groupe donné de trames, informe le générateur de code de ce que le code analysé est le bon ou non, cette dernière interprétation entraînant l'analyse d'un autre code de cryptage.

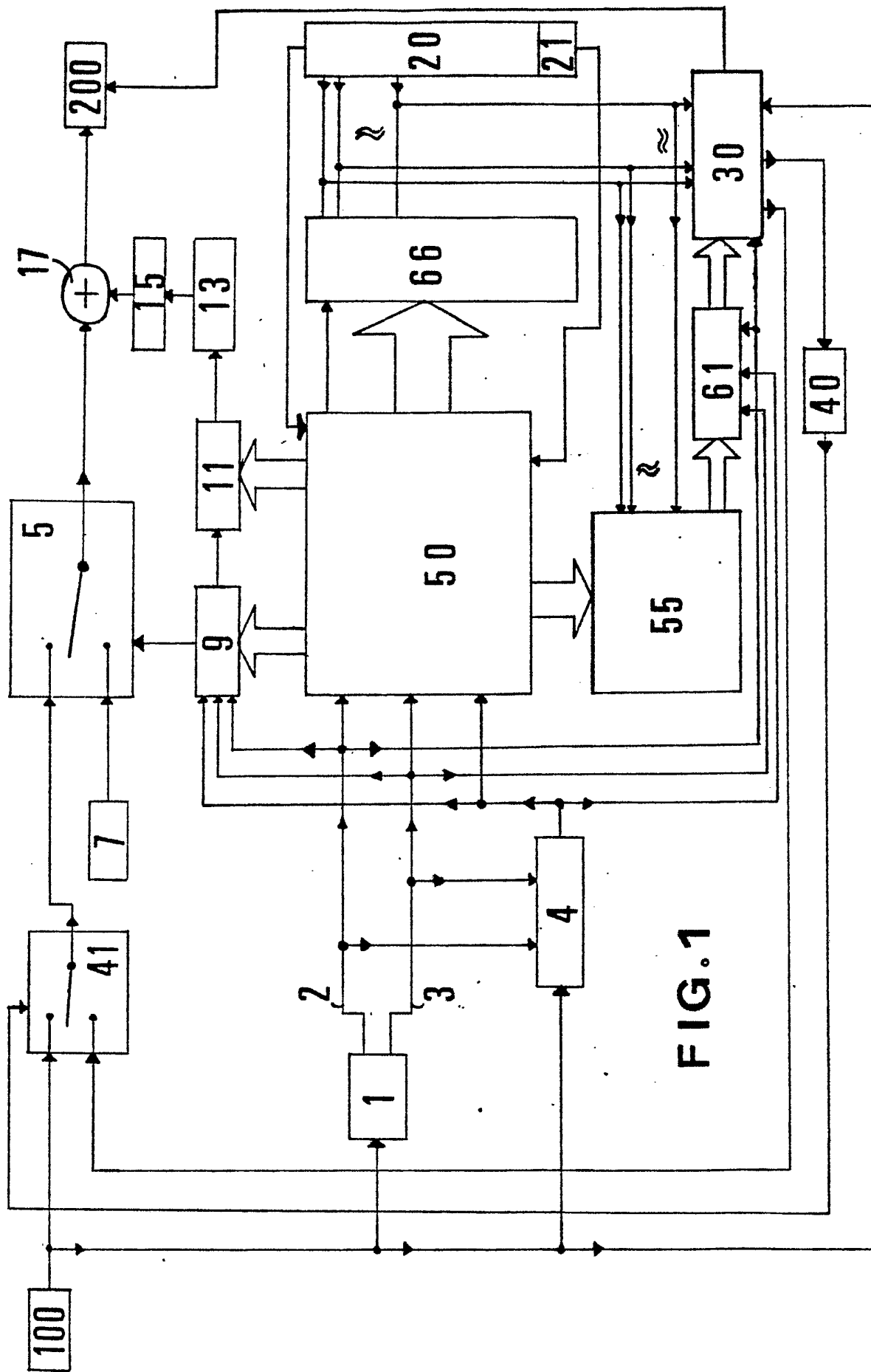


FIG. 1

FIG. 2

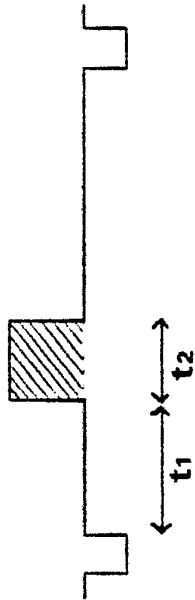
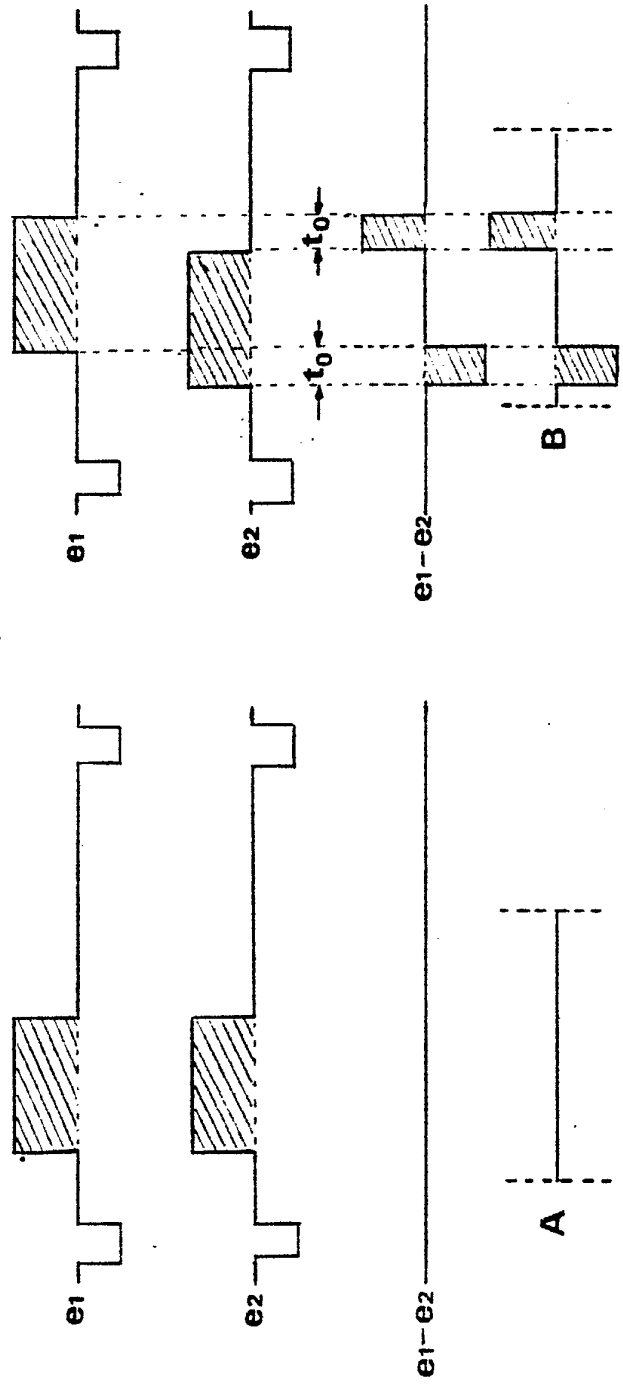


FIG. 4



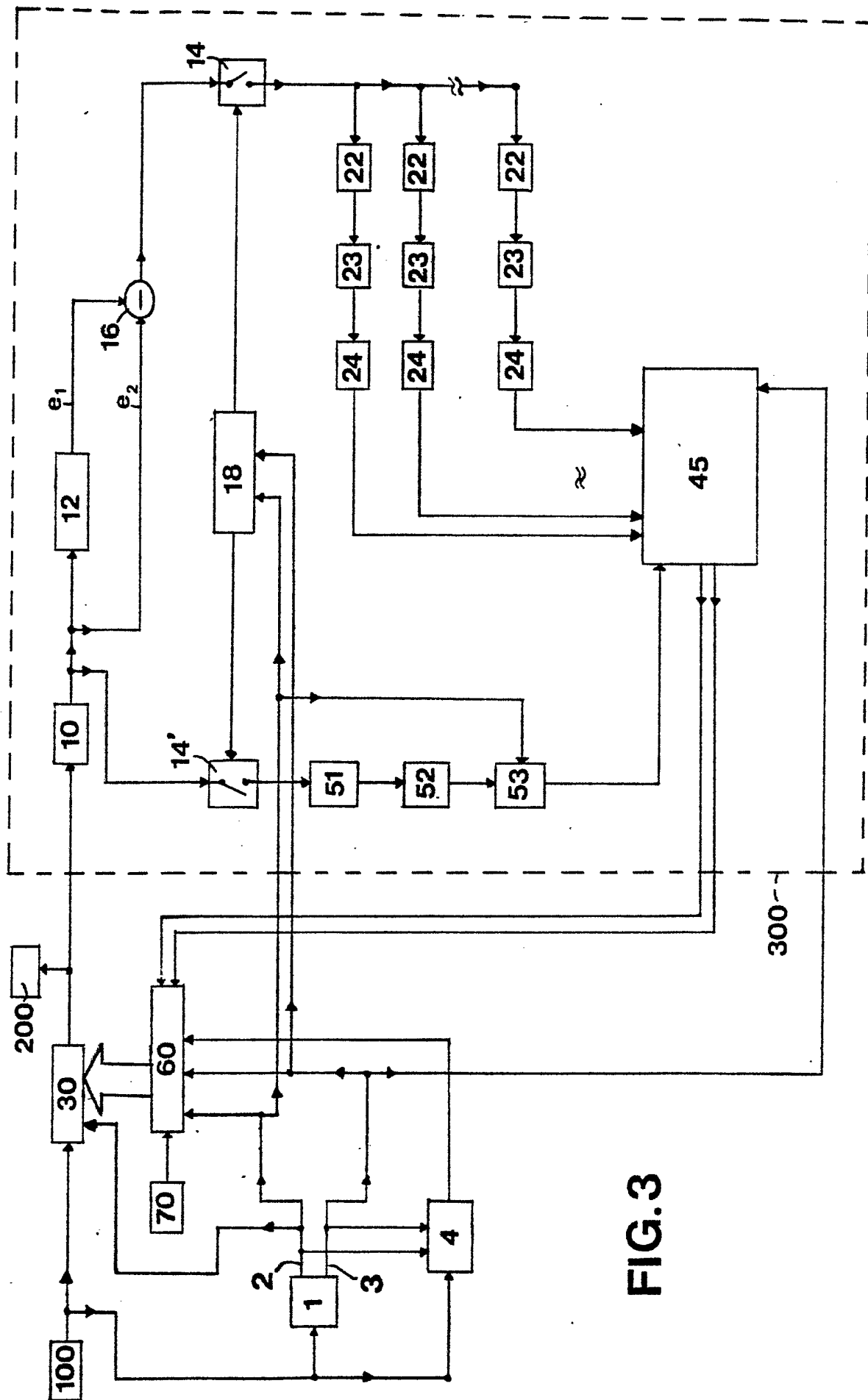


FIG. 3

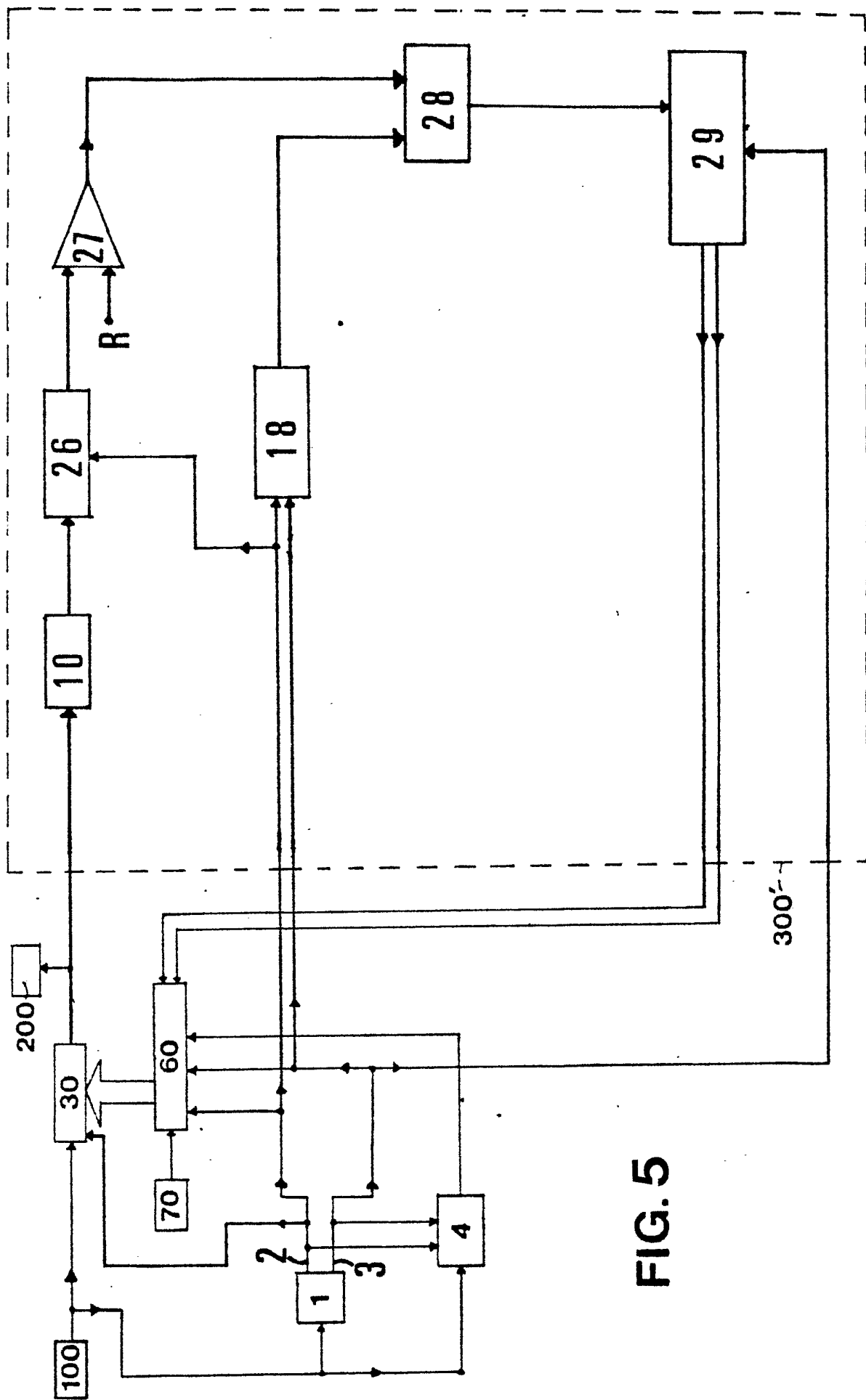


FIG. 5

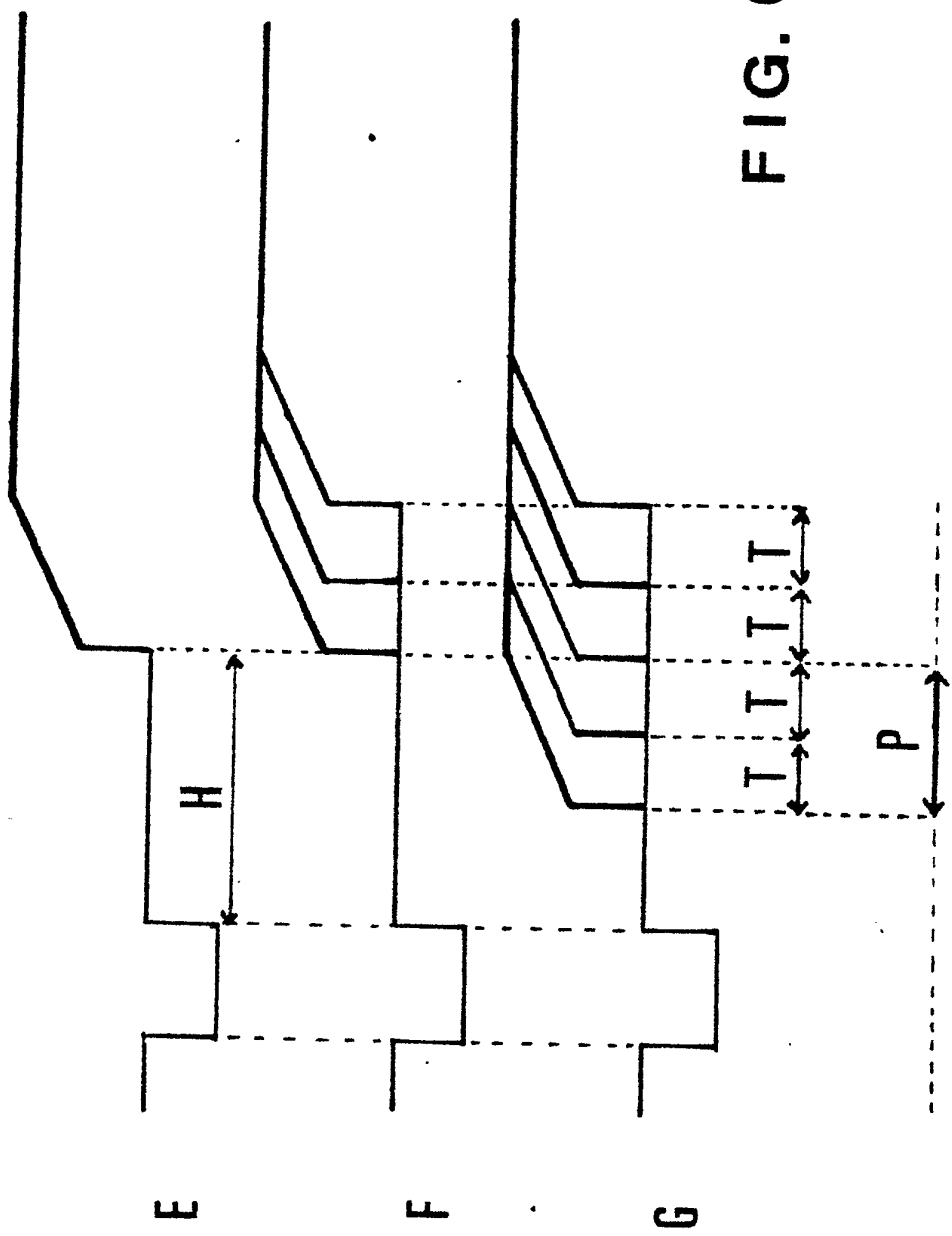


FIG. 6