



CONFÉDÉRATION SUISSE

OFFICE FÉDÉRAL DE LA PROPRIÉTÉ INTELLECTUELLE

⑪ CH 664 658 A5

⑤① Int. Cl.4: H 04 N 7/167

Brevet d'invention délivré pour la Suisse et le Liechtenstein

Traité sur les brevets, du 22 décembre 1978, entre la Suisse et le Liechtenstein

⑫ **FASCICULE DU BREVET** A5

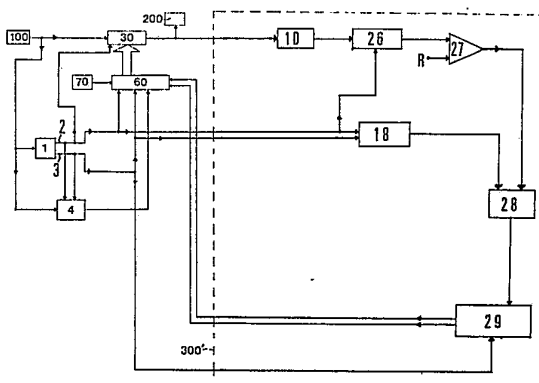
⑮ Numéro de la demande: 1289/85

⑳ Date de dépôt: 22.03.1985

㉔ Brevet délivré le: 15.03.1988

④⑤ Fascicule du brevet
publié le: 15.03.1988⑦③ Titulaire(s):
Technical Developments and Investments, Eschen
(LI)⑦② Inventeur(s):
Zberg, François J., Pont-la-Ville⑦④ Mandataire:
Kirker & Cie SA, Genève⑤④ **Procédé et dispositif d'analyse et de reconnaissance automatique du code de cryptage d'émissions de télévision.**

⑤⑦ Le procédé d'analyse et de reconnaissance automatique consiste à tester successivement chacun des différents codes de cryptage possibles par l'analyse, pour chacun de ces codes, d'un certain nombre de trames obtenues à l'aide d'un décodeur adapté fonctionnant sur la base de ce code, et pour chacune de ces trames de certaines lignes la composant, l'analyse se faisant par l'étude de la présence d'un signal image sur une plage donnée (P) du palier de suppression (H) normalement réservé à la référence de noir. Cette analyse se fait successivement pour chaque code jusqu'à obtention, pour un code donné, d'une série de trames pour lesquelles moins d'un nombre déterminé des lignes prises en compte dans l'analyse ne débutent leur signal image sur la plage du palier de suppression choisie pour l'analyse. Le dernier code représente le code recherché.



REVENDECATIONS

1. 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, 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., jusqu'à ce que le code de cryptage généré à l'aide du décodeur des lignes, dont celles prises en compte dans l'analyse, et pour un groupe déterminé de trames, ne débutent 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.

2. Dispositif pour la mise en œuvre 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 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 couleurs, 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.

DESCRIPTION

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 brevet suisse N° 661 628 (demande déposée le 9 janvier 1985 par Technical Developments & Investments) décrit différents procédés et dispositifs d'analyse et de reconnaissance du code de cryptage d'émissions de télévision, dont la présente invention ne représente qu'une autre forme, plus simple, d'analyse et de reconnaissance automatique du code de cryptage d'émissions de télévision.

Le but de l'invention est d'arriver à déterminer le cycle pseudo-aléatoire des décalages utilisés 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, cela 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 N° 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 T1, T2, T3 avec, par exemple, T1 = 0, T2 = s, T3 = 2 s et avec s = 1 µs).

Il faut enfin que le nombre des différents codes pseudo-aléatoires possibles ne soit pas infini.

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

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 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 déterminé 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-elle 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 différences 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 2 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 1 représente un dispositif d'analyse et de reconnaissance automatique du code de cryptage mettant en œuvre le 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 couleurs 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 la 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 utilisés, pendant le temps d'utilisation respectif, à un décodeur adapté, pour obtenir une image parfaitement décryptée de la version cryptée de départ.

- Les procédé et dispositif selon l'invention peuvent être également utilisés pour la recherche du code de cryptage lorsque les émissions de télévision non seulement sont cryptées comme indiqué dans le préambule de la revendication 1, mais également appliquent 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 par un circuit simple, et le signal être restitué corrigé de cette inversion de polarité, ce qui permet d'appliquer les procédé et dispositif de la pré-

sente 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.

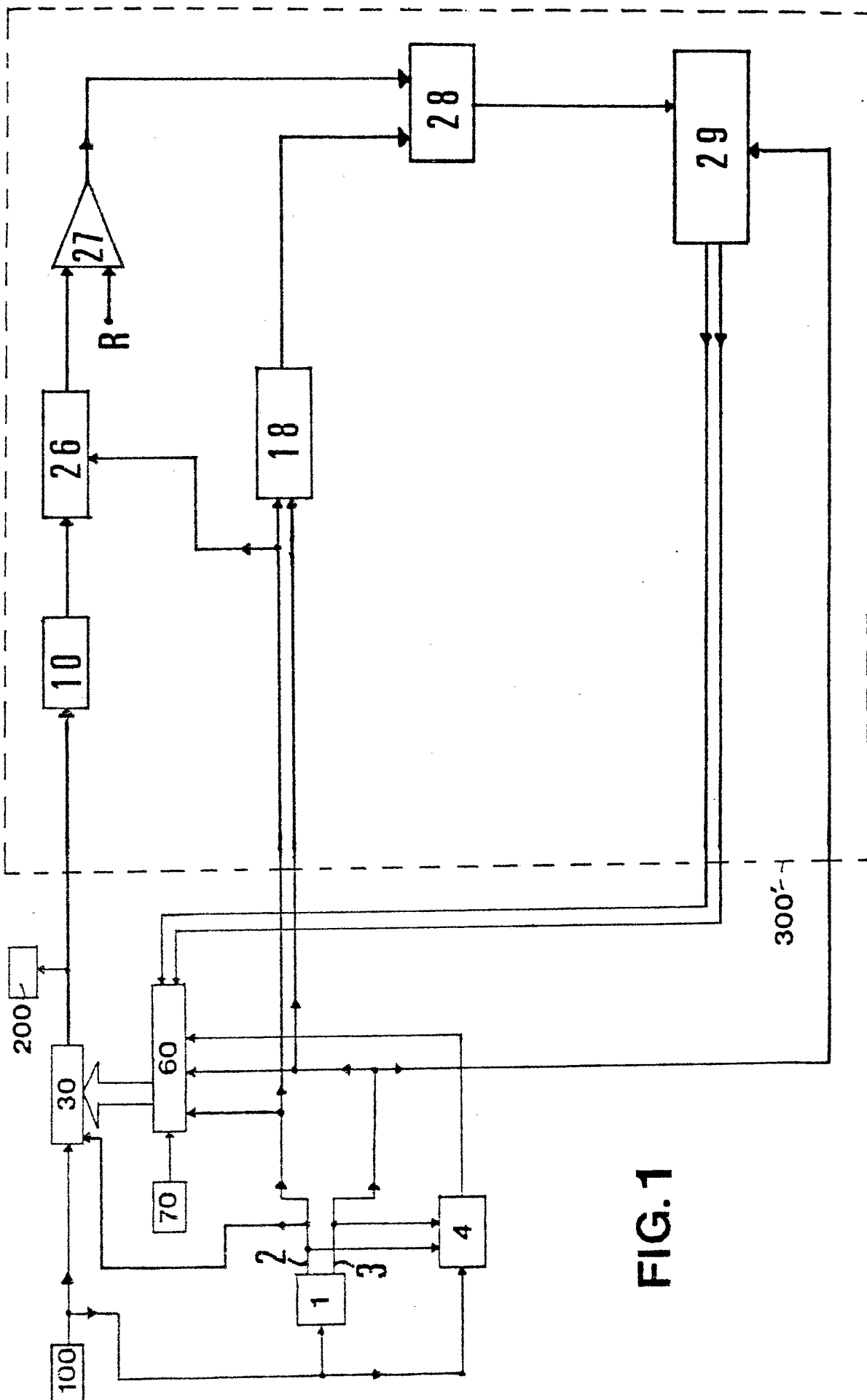


FIG. 1

