(19) RÉPUBLIQUE FRANÇAISE

INSTITUT NATIONAL
DE LA PROPRIÉTÉ INDUSTRIELLE

PARIS

(11) N° de publication : **2 530 101**
(à n'utiliser que pour les commandes de reproduction)

(21) N° d'enregistrement national : **82 11841**

(51) Int Cl³ : H 04 K 1/04; H 04 N 7/16.

(12) DEMANDE DE BREVET D'INVENTION A1

(22) Date de dépôt : 6 juillet 1982.

(30) Priorité

(43) Date de la mise à disposition du public de la demande : BOPI « Brevets » n° 2 du 13 janvier 1984.

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

(71) Demandeur(s) : *Société dite : THOMSON-BRANDT, société anonyme.* -- FR.

(72) Inventeur(s) : Jean-Claude Guillon, Jean-Michel Levesque, Alain Poirel et Jean-Yves Moraillon.

(73) Titulaire(s) :

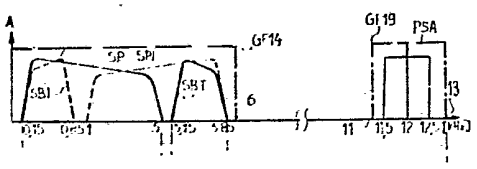
(74) Mandataire(s) : Philippe Guilguet.

(54) Procédé et système de transmission cryptée d'un signal, notamment audio-fréquence.

(57) L'invention concerne un procédé et un système pour la mise en œuvre de celui-ci, destiné à la transmission cryptée (codée) d'un signal, notamment d'un signal audio-fréquence.

Le procédé de l'invention comprend une partie de cryptage dans lequel un signal clair est d'abord préaccentué, ensuite on lui ajoute en bout de bande un signal de brouillage qui est constitué par la partie basse-fréquence de son spectre transposée au-delà de sa fréquence maximale. Le signal somme qui est ainsi rendu inintelligible, est alternativement transmis avec un spectre normal et un spectre inversé, obtenu par la modulation d'amplitude d'une porteuse dont la fréquence est supérieure à celle du spectre du signal somme, selon une suite ou séquence pseudo-aléatoire composée de signaux rectangulaires dont la durée et l'écart entre deux signaux successifs, sont variables de façon aléatoire. Il comprend également une partie de décryptage, dans laquelle le signal somme au spectre inversé est démodulé de manière synchrone afin de le réinverser et dans laquelle le signal alternativement normal et réinversé est filtré pour en éliminer le signal de brouillage et ensuite désaccentué pour restituer le signal clair.

Application à la transmission de signaux sonores à un auditoire autorisé d'abonnés ou par péage.



FR 2 530 101 - A1

PROCEDE ET SYSTEME DE TRANSMISSION CRYPTEE D'UN SIGNAL, NOTAMMENT AUDIO-FREQUENCE

La présente invention concerne un procédé et un système de transmission cryptée (brouillée ou codée) d'un signal, notamment audio-fréquence, du type dans lequel celui-ci est encrypté de manière prédéterminée, avant son émission par voie hertzienne ou par réseau câblé, de telle sorte qu'il soit rendu inintelligible à tout récepteur dépourvu d'un dispositif de décryptage adapté qui permet de le restituer dans sa forme initiale. En résumé, un système de "cryptage" ou de transmission cryptée ou codé d'un signal audio-fréquence clair d'entrée comprend principalement, à l'émission, en aval de sa source et en amont de la sortie qui peut être constituée par l'entrée d'un modulateur, un dispositif d'encryptage qui le reçoit et qui fournit un signal crypté ou codé et, à la réception, un dispositif de décryptage qui reçoit ce dernier et fournit un signal clair correspondant au moins sensiblement au signal d'entrée.

Divers systèmes de cryptage qui permettent d'interdire l'accès à l'information aux personnes non autorisées, c'est-à-dire à ceux dont les récepteurs ne sont pas munis de dispositifs de décryptage adaptés, soit afin de conserver le secret ou le caractère privé du message, soit afin de n'autoriser que des personnes abonnées ou soumises au péage d'une taxe à le recevoir en clair, sont bien connus et présentent respectivement des complexités correspondant sensiblement au degré d'inviolabilité désirée.

La présente invention a, plus particulièrement, pour objet un procédé et des dispositifs de cryptage et de décryptage fréquentiel respectifs d'un signal audio-fréquence dont la bande passante s'étend de 150 Hz à 5 kHz environ et un procédé de décryptage dont la mise en oeuvre est relativement aisée, afin que le coût d'un dispositif de

décryptage le rende accessible à une diffusion dans le grand public (transmission de signaux numériques ou analogiques, tels que des signaux sonores constituant partie, par exemple, des signaux de télévision à péage ou par abonnement), tout en assurant une protection du message (son inaccessibilité à des tiers non autorisés qui n'ont pas reçu de son diffuseur de décrypteurs prévus à cet effet) convenable.

Un procédé simple de cryptage de type fréquentiel d'un signal analogique audio-fréquence, elaboré par la demanderesse, consisterait en la transmission alternée, selon une suite "pseudo-aléatoire", du signal avec un spectre normal et avec un spectre inversé qui peut être obtenu, par exemple, en modulant une onde porteuse de fréquence peu supérieure à la fréquence maximale du spectre, en amplitude par le signal analogique à transmettre et en faisant passer la porteuse modulée par un filtre passe-bas ou passe-bande qui ne laisserait passer que la bande latérale inférieure. Une suite pseudo-aléatoire (dite "pseudo-random sequence" en anglais) est composée d'une succession de signaux rectangulaires dont les durées et celles des intervalles qui les séparent, varient de façon aléatoire. Des moyens composés d'une combinaison de circuits intégrés logiques disponibles dans le commerce (horloges, basculeurs, compteurs, registres à décalage, portes "ET" et "OU", etc.) permettent de réaliser aisément des générateurs de suites pseudo-aléatoires. Une telle inversion alternée du spectre ne constitue pas un procédé de cryptage inviolable, car l'énergie de chacune des composantes (harmoniques élevées) du spectre d'un signal sonore diminue avec l'augmentation de son rang, c'est-à-dire de sa fréquence, et l'inversion peut être détectée au moyen d'un filtre passe-bande sélectif à travers un détecteur de crête et un éventuel comparateur de tension à seuil (basculeur de Schmitt) permettrait de restituer la suite pseudo-aléatoire commandant l'alternance de l'inversion.

Les procédé et système de transmission cryptée, objets de l'invention, permettent de palier à cet inconvénient. Dans ceux-ci, en effet, le signal audio-fréquence est soumis à l'émission à une

préaccentuation qui renforce ses composantes aux fréquences élevées et on lui adjoint en bout de bande, dans le mode de réalisation préféré, la partie basse-fréquence de son propre spectre qui est ainsi transposée au-delà de ses fréquences plus élevées et qui joue le rôle d'un signal de brouillage et de camouflage (l'énergie du spectre du signal résultant est comparable à ses deux extrémités opposées).

Le procédé objet de l'invention comprend un procédé d'encryptage destiné à transformer un signal clair en un signal inintelligible et un procédé de décryptage destiné à tranformer ce dernier en un signal suffisament semblable au signal clair pour être intelligible.

Suivant l'invention, le procédé d'encryptage d'un signal clair consiste à préaccentuer celui-ci, à ajouter au signal préaccentué un signal de brouillage dont le spectre se situe au-delà de la fréquence maximale de celui du signal préaccentué pour obtenir un signal somme, à inverser le spectre de celui-ci par la modulation d'amplitude d'une porteuse d'inversion dont la fréquence est située au-dessus de la fréquence maximale du spectre du signal somme et à transmettre le signal somme alternativement avec les spectres normal et inversé, l'alternance étant commandée au moyen d'une suite pseudo-aléatoire.

Egalement suivant l'invention, le procédé de décryptage consiste à démoduler le signal somme au spectre alternativement normal et inversé, de manière synchrone au moyen d'une porteuse de réinversion asservie en phase et en fréquence à celle d'inversion, à transmettre alternativement, selon la même suite pseudo-aléatoire reçue par ailleurs, le signal somme reçu et celui après démodulation synchrone, à un filtre passe-bas éliminant le signal de brouillage et à désaccentuer le signal issu de ce filtre passe-bas.

Un autre objet de l'invention est un système permettant la mise en oeuvre des procédés décrits ci-dessus.

L'invention sera mieux comprise et d'autres de ses objets, caractéristiques et avantages ressortiront de la description qui suit et des dessins annexés, s'y rapportant, sur lesquels :

- la figure 1 représente le spectre du signal audio-fréquence (l'enveloppe de celui-ci) clair ;

- la figure 2 représente le spectre du signal en bande de base après préaccentuation ;

- la figure 3 représente le spectre du signal de brouillage obtenu par filtrage passe-bas à partir du signal préaccentué de la figure 2 ;

- la figure 4 représente le spectre du signal de brouillage modulant une sous-porteuse en amplitude ;

- la figure 5 représente le spectre du signal transmis résultant de l'addition au signal préaccentué de la bande latérale supérieure du signal de brouillage transposé au-delà de la fréquence maximale du spectre du premier ;

- la figure 6 représente le spectre d'une porteuse de 6 kHz modulée en amplitude par le signal somme résultant de l'addition du signal de brouillage au signal préaccentué, qui permet l'inversion du spectre ;

- la figure 7 représente le spectre inversé obtenu par l'élimination de la porteuse et des bandes latérales supérieures du produit de modulation de la figure 6 ;

- la figure 8 représente les spectres respectifs des deux signaux transmis de manière alternée selon la suite pseudo-aléatoire ;

- la figure 9 représente le spectre du signal inversé résultant d'une démodulation synchrone ;

- la figure 10 représente le spectre du signal clair restitué après filtrage et désaccentuation, fourni par la sortie du dispositif de décryptage ;

- la figure 11 est un diagramme de la forme d'onde de tension (en fonction du temps) d'une suite pseudo-aléatoire commandant la transmission alternée (consécutive) du signal somme au spectre normal de la figure 5 et au spectre inversé de la figure 7 ;

- la figure 12 est un schéma synoptique d'un mode de réalisation du dispositif d'encryptage du système de transmission cryptée selon l'invention ; et

- la figure 13 est un schéma synoptique d'un mode de réalisation du dispositif de décryptage de ce sytème, adapté pour coöpérer avec un dispositif d'encryptage de la figure 12.

Sur la figure 1, on a représenté l'enveloppe des composantes du spectre d'un signal audio-fréquence clair SC qui est compris entre 0,15 à 5 kHz et dont les amplitudes A respectives décroissent avec la fréquence. Ce signal est fourni par une source représentée en 1 sur la figure 12 qui est un schéma synoptique d'un dispositif d'encryptage 10. Le signal clair SC est appliqué à l'entrée d'un filtre de préaccentuation 2 de type dont le gain ou la fonction de transfert augmente avec la fréquence (connu des techniques de la modulation de fréquence). Le filtre de préaccentuation 2 qui favorise la transmission des fréquences plus élevées, fournit un signal préaccentué SP dont le spectre est illustré par la figure 2. Ce signal préaccentué SP est appliqué, d'une part, à une première entrée 30 d'un premier additionneur analogique 3 et, d'autre part, à l'entrée d'un filtre passe-bas 4 qui ne transmet que la partie basse-fréquence (de 150 à 850 Hz) du spectre du signal préaccentué SP, qui sera utilisée ici en tant que signal de brouillage SB dont le spectre est représenté sur la figure 3. Le signal de brouillage SB est appliqué à l'entrée de modulation 50 d'un premier modulateur d'amplitude 5 dont l'entrée de porteuse 51 reçoit une onde porteuse de 5 kHz (c'est-à-dire de fréquence égale à la fréquence maximale du spectre du signal préaccentué) d'une source (oscillateur, par exemple) constituée ici par une horloge (H) 7 fournissant une onde de 60 kHz connectée en cascade avec un diviseur de fréquence par douze 6. La sortie 52 du premier modulateur 5 fournit un signal dont le spectre comprend une bande latérale inférieure BLI (inversée par rapport au spectre de SB), la porteuse dite de brouillage PB et une bande latérale supérieure BLS s'étendant de 5,15 à 5,85 kHz, c'est-à-dire transposée de 5 kHz vers le haut par rapport au signal de brouillage à la sortie du filtre passe-bas 4. On obtient ainsi que l'écart entre la fréquence maximale du spectre du signal préaccentué SP et la fréquence minimale de celui de la bande latérale supérieure (BLS) est sensiblement égale à la fréquence minimale de la bande de base.

Le signal de sortie du modulateur 5 est appliqué à l'entrée d'un filtre passe-bande 8 qui n'en transmet que la bande latérale supérieure (BLS, figure 4) située au-delà de la fréquence maximale (5 kHz) du signal préaccentué SP.

La sortie du filtre passe-bande 8 est reliée à la seconde entrée 31 de l'additionneur analogique 3 de façon à ajouter au signal préaccentué SP, le signal de brouillage transposé SBT.

Le signal "somme" à la sortie du premier additionneur 3 présente alors un spectre illustré par la figure 5. Ce dernier signal est appliqué, d'une part, à une première entrée de signal 90 d'un commutateur électronique rapide 9 et d'autre part, à l'entrée de modulation 110 d'un second modulateur d'amplitude 11. L'entrée de porteuse 111 du second modulateur 11 reçoit d'une autre source d'oscillations, une seconde porteuse à la fréquence de 6 kHz, afin qu'elle soit située en dehors du spectre du signal somme SP + SBT que fournit le premier additionneur 3.

La seconde source comprend en cascade l'horloge (H) 7, un second diviseur par cinq 12 fournissant une onde à 12 kHz et un troisième diviseur par deux 13 fournissant l'onde porteuse à 6 kHz.

Le spectre du signal fourni par le second modulateur 11, illustré par la figure 6 comprend, en allant des fréquences inférieures vers les supérieures, une bande latérale inférieure composée du signal de brouillage inversé SBI (de 150 à 850 Hz) et du signal préaccentué transposé et également inversé SPI (de 1 à 5,85 kHz), la seconde porteuse de modulation dite d'inversion PMI (6kHz) et une bande latérale supérieure composée du signal préaccentué transposé (de 6,15 à 11 kHz) et du signal de brouillage également transposé (de 11,15 à 11,85 kHz).

La sortie du second modulateur 11 est relié à un second filtre passe-bas 14 qui élimine la second porteuse PMI à 6 kHz et la bande latérale supérieure (de 6,15 à 11,85 kHz) et ne transmet que le spectre du signal somme inversé comprenant le signal de brouillage inversé SBI et le signal préaccentué inversé SPI, illustré par la figure 7, à la seconde entrée 91 du commutateur 9. La sortie 92 de

ce dernier fournit donc alternativement le signal somme (SP + SBT, figure 5) normal et le signal somme au spectre inversé (SBI + SPI, figure 7) autour de la seconde fréquence porteuse PMI de 6 kHz, suivant le niveau du signal V_{93} appliqué à son entrée de commande de commutation 93.

Ce signal V_{93} est constitué par une suite pseudo-aléatoire SPA dont la forme d'onde de tension a été illustrée sur la figure 11 et qui a été élaboré dans un générateur de signaux pseudo-aléatoires (GPA) 16 qui peut être piloté par une horloge interne (à la fréquence de 10 Hz, par exemple). La suite pseudo-aléatoire V_{93} (SPA) est un signal à deux niveaux (binaire) dont la durée des états successifs varie de manière aléatoire selon un code prédéterminé par l'agencement de ses moyens d'élaboration pouvant comporter des circuits intégrés logiques (numériques), tels que des compteurs-diviseurs, des registres à décalage, des portes logiques ET, OU et OU exclusif et des liaisons de rebouclage diversement agencées pour élaborer une séquence déterminée (connu du domaine des télécommunications par satellites et du cryptage des messages binaires ou audio-fréquence).

Afin de pouvoir établir une corrélation à la réception et de restituer au moins approximativement le signal clair initial, il faut également transmettre un signal correspondant à la suite pseudo-aléatoire qui devra être difficile de détecter à partir du contenu du signal transmis. Ceci est effectué en modulant une troisième porteuse de 12 kHz PSA fournie par le diviseur par cinq 12, en amplitude, soit directement par la suite pseudo-aléatoire SPA ce qui faciliterait la violation de la confidentialité du message, car il suffirait de disposer d'un bon analyseur de spectre basse-fréquence pour déterminer sa fréquence, soit par un signal correspondant, codé à l'aide d'un transcodeur 17 (en pointillé).

La sortie du diviseur par cinq 12 est à cette fin reliée à l'entrée de porteuse 181 d'un troisième modulateur d'amplitude 18 dont l'entrée du signal 180 reçoit du transcodeur 17 un signal binaire caractérisant la suite pseudo-aléatoire SPA. La sortie du troisième modulateur 18 est reliée à l'entrée d'un second filtre passe-bande 19

qui limite la largeur des bandes latérales à plus et moins 1 kHz autour de 12 kHz.

La sortie 92 du commutateur 9 est reliée à la première entrée 150 d'un second additionneur analogique 15 et celle du second filtre passe-bande 19 à la seconde entrée 151 de ce dernier. Le second additionneur 15 fournit donc sur sa sortie 152 reliée à la sortie 20 du dispositif d'encryptage 10 un spectre tel qu'illustré par la figure 8, qui comprend alternativement le signal somme normal (SP + SBT) et le signal somme au spectre inversé (SBI + SPI), représenté par des tirets, que laisse passer le filtre 14 dont le gabarit GF 14 est représenté par des traits mixtes, et la troisième porteuse PSA avec ses bandes de modulation qui sont transmis par le filtre 19 au gabarit GF 19 (également illustré à l'aide de traits mixtes à droite de la figure 8). La sortie 20 est reliée à l'entrée d'une voie de transmission hertzienne (ou par câbles ou même en multiplex avec d'autres signaux).

La figure 13 illustre sous la forme d'un schéma synoptique, un dispositif de décryptage permettant de restituer, à partir du signal fourni par la sortie 20 du dispositif d'encryptage 10 dont le spectre est illustré sur la figure 8, un signal audio-fréquence clair et intelligible, correspondant au moins sensiblement à celui fourni par source (dont le spectre est illustré par la figure 1).

Le dispositif de décryptage 30 comporte une entrée 21 qui reçoit de la sortie de la voie de transmission hertzienne (démodulateur) ou par câble (démultiplexeur, par exemple), non représentée, le signal dont le spectre a été illustré par la figure 8.

Cette entrée 21 recevant le signal crypté alimente, d'une part, l'entrée d'un troisième filtre passe-bas 22 dont le gabarit correspond à celui du second GF 14 de la figure 8 et, d'autre part, un troisième filtre passe-bande 23 qui permet de séparer la troisième porteuse PSA à 12 kHz du reste du signal crypté et dont le gabarit correspond également à celui GF 19 de la figure 8.

La sortie du filtre passe-bas 22 alimente, d'une part, une première entrée 240 d'un second commutateur analogique 24 qui doit

relier celle-ci à sa sortie 242, lorsque l'on transmet le signal normal SP + SBT (non inversé, voir spectre de la figure 5) et, d'autre part, l'entrée de signal 250 d'un démodulateur synchrone 25 dont la sortie 252 fournit un spectre du type illustré sur la figure 9. Pour obtenir ceci, un oscillateur local 26 fournissant sur sa sortie 265 une onde porteuse dont la fréquence est égale (6 kHz) à celle de la seconde PMI qui effectue à l'émission l'inversion du signal, doit alimenter l'entrée de porteuse 251 du démodulateur synchrone 25. On notera ici qu'un tel démodulateur synchrone 25 est analogue à un modulateur, tel que ceux 5, 11 et 18 de la figure 12.

Cet oscillateur local 26 qui peut également servir à synchroniser la restitution de la suite pseudo-aléatoire SPA (V_{93} de la figure 11), comprend une boucle à verrouillage de phase (PLL) composée d'un oscillateur à fréquence commandée par tension 263 (appelé "voltage-controlled oscillator" ou "VC0" en anglais), d'un comparateur de phase 261 recevant, d'une part, la troisième porteuse modulée PSA fournie par la sortie du troisième filtre passe-bande 23 à travers l'entrée de synchronisation 260 de l'oscillateur local 26 et d'autre part, l'onde fournie par le VC0 263, d'un quatrième filtre passe-bas 262 qui reunit la sortie du comparateur de phase 261 à l'entrée de commande de la fréquence par une tension du VC0 263 qui fournit alors une onde de 12 kHz synchronisée avec la troisième porteuse PSA. Pour obtenir une onde de 6 kHz, l'onde fournie par le VC0 263 est appliquée à l'entrée d'un quatrième diviseur de fréquence par deux 264 dont la sortie constitue celle 265 des sorties de l'oscillateur local 26 qui alimente l'entrée de porteuse 251 du démodulateur sychrone 25 par une quatrième porteuse de démodulation inversée PDI (figure 9).

La sortie 252 du démodulateur 25 est reliée à l'entrée d'un cinquième filtre passe-bas 27 qui élimine la quatrième porteuse PDI et les bandes latérales supérieures, c'est-à-dire sensiblement tout au-dessus de 5,85 kHz. Dans ce cas, le signal de sortie du cinquième filtre passe-bas 27 ne comprend que le spectre du signal préaccentué SP et celui de brouillage transposé SBT. Il est évident qu'il

est déjà possible d'éliminer le signal de brouillage transposé SBT à ce niveau en choisissant une fréquence de coupure haute (- 50 dB) de ce filtre 27 située entre 5 et 5,15 kHz. Dans ce cas il est avantageux d'insérer un filtre passe-bas analogue entre la sortie du troisième filtre 22 et la première entrée de signal 240 du second commutateur analogique 24.

La sortie du cinquième filtre passe-bas 27 est reliée à la seconde entrée de signal 241 du second commutateur 24 afin de lui fournir la portion du spectre du signal démodulé de manière synchrone, qui est inférieure à la fréquence de la porteuse de démodulation PDI, c'est-à-dire que pendant la transmission du signal inversé SBI + SPI (figure 7), cette entrée 241 reçoit un signal sensiblement analogue au signal normal SP + SBT (figure 5).

La synchronisation des deux commutateurs 9 et 24 est effectuée à l'aide du signal modulant la troisième porteuse PSA (figure 8) qui après sa démodulation d'amplitude (synchrone ou non) dans un démodulateur 28, est constitué par des signaux binaires qui sont soit directement, soit à travèrs un décodeur 29 effectuant l'opération inverse de celle du transcodeur 17 à l'émission, appliquées à l'entrée de commande 243 du second commutateur 24.

La sortie 242 du second commutateur 24 est reliée à l'entrée d'un sixième filtre passe-bas 31 qui, comme il a été dit précédemment, pourrait également être inséré entre la sortie du troisième filtre passe-bas 22 et l'entrée 240 du second commutateur 24 et qui permet d'éliminer le signal de brouillage transposé SBT en présentant une fréquence de coupure haute située entre 5 et 5,15 kHz. La sortie du sixième filtre passe-bas 31, ou celle 242 du second commutateur, alimente un filtre de désaccentuation 32 dont le gain décroît avec la fréquence de manière inverse à la croissance de celui du filtre de préaccentuation 2 du dispositif d'encryptage 10 de la figure 12.

On notera ici que si le filtre de désaccentuation 32 présente une coupure franche (- 50 dB ou plus d'atténuation), on peut faire l'économie des cinquième 27 et sixième 31 filtres passe-bas. Plus

précisément dans le mode de réalisation préféré du dispositif de décryptage 30, le cinquième filtre passe-bas 27 situé en aval du démodulateur synchrone 25, est omis et le sixième filtre passe-bas 31 est combiné avec le filtre de désaccentuation 32 en un dispositif de filtrage unique, réalisable de manière classique.

Le filtre de désaccentuation 32 dont le gabarit GF 32 est représenté sur la figure 10 en traits mixtes, fournit sur sa sortie reliée à celle 33 du dispositif de décryptage un signal audio-fréquence clair, restitué SCR (à quelques produits de distorsion et d'intermodulation près) dont le spectre, analogue à celui de la figure 1, est également illustré sur la figure 10.

On notera ici que pour la transmission alternée des signaux somme normal (SP + SBT) et inversé (SBI + SPI) dont on voit respectivement les spectres sur les figures 5 et 7 ou ensemble sur la figure 8, il suffit de transmettre la seconde porteuse d'inversion PMI de 6 kHz avec une modulation d'amplitude correspondant à la suite pseudo-aléatoire, transcodée ou non. Toutefois, dans ce cas les transitions entre les niveaux des signaux binaires auront des pentes réduites puisque les bandes latérales devront être limitées en largeur à 100 Hz environ. Cet inconvénient pourrait être palié par l'utilisation exclusive de la bande latérale supérieure avec la porteuse PMI, pour transmettre le signal de synchronisation de la commutation, selon les techniques BLU (bande latérale unique) bien connus du technicien des télécommunications. Dans ce cas, le filtre passe-bande 23 séparant la porteuse PSA du reste du signal devra présenter une courbe de sélectivité idoïne.

Il est également à remarquer ici que l'utilisation des techniques numériques pour la mise en oeuvre du procédé de transmission cryptée ne sort pas du domaine de la présente invention. Cette application des techniques numériques permettant l'utilisation de circuits intégrés logiques peut être limitée au traitement du signal transmis présent à l'entrée 21 du dispositif de décryptage 30 (voir figure 13), la boucle à verrouillage de phase 26 continuera d'être alimentée à travers un filtre passe-bande analogique séparant la

sous-porteuse ou porteuse PSA modulée. L'avantage des techniques numériques est l'absence de réglages et de composants bobinés, ainsi que l'intégrabilité de l'ensemble qui, malgré un nombre d'éléments actifs plus élevé, résulterait en un coût à l'unité moindre pour les grandes séries.

Le procédé de cryptage objet de l'invention peut également être appliqué à des signaux autres que ceux aux fréquences sonores. Toutefois, il faudra dans ce cas utiliser des composants actifs plus rapides ou de fréquence de transition plus élevée.

On notera également que le signal de brouillage n'est pas obligatoirement constitué par la partie basse-fréquence du signal préaccentué, mais peut être engendré par d'autres générateurs de bruit, tel qu'un oscillateur à fréquence variable, commandée au moyen d'un signal basse-fréquence ou d'une forme d'onde à variations linéaires, par exemple.

Il est également possible de transmettre la suite pseudo-aléatoire (SPA) ou un signal résultant de son transcodage, par câble, par exemple téléphonique, à des abonnés, afin d'obtenir une diffusion restreinte du signal audio-fréquence.

REVENDICATIONS

1. Procédé de transmission cryptée d'un signal, notamment d'un signal audio-fréquence, dans lequel l'encryptage de type fréquentiel est effectué par l'inversion alternée de son spectre selon une suite pseudo-aléatoire, caractérisé en ce que le signal clair est soumis à une préaccentuation de façon à favoriser la transmission des composantes de son spectre aux fréquences élevées, en fonction de leur fréquence, préalablement à l'inversion de son spectre.

2. Procédé de transmission cryptée suivant la revendication 1, caractérisé en ce que, préalablement à l'inversion, on ajoute en bout de bande au spectre du signal préaccentué, un signal de brouillage dont le spectre comprend une fréquence minimale supérieure à la fréquence maximale de celui du signal préaccentué et en ce que l'inversion du spectre du signal somme ainsi obtenu est effecutée au moyen d'une porteuse dont la fréquence est supérieure à la fréquence maximale du spectre du signal de brouillage.

3. Procédé de transmission cryptée suivant la revendication 2, caractérisé en ce que le signal de brouillage est obtenu par la séparation de la partie basse-fréquence du signal préaccentué et par la transposition de celle-ci au-delà de la fréquence maximale de son spectre, en modulant en amplitude une porteuse dont la fréquence est égale ou supérieure à cette dernière et en ajoutant à ce spectre, la bande latérale supérieure résultant de cette modulation, qui est obtenue par un filtrage passe-bande.

4. Procédé de transmission cryptée suivant l'une des revendications précédentes, caractérisé en ce que l'on transmet, outre le signal préaccentué ou le signal somme au spectre alternativement inversé, une autre porteuse dont la fréquence est située au-dessus de la fréquence maximale de ce spectre et égale à un multiple entier de la porteuse utilisée pour l'inversion.

5. Procédé de transmission cryptée suivant la revendication 4, caractérisé en ce que, à l'encryptage, l'autre porteuse est modulée en amplitude par un signal correspondant à la suite pseudo-aléatoire.

6. Procédé de transmission cryptée suivant l'une des revendications précédentes, dans lequel le décryptage comprend la réinversion du spectre inversé de manière alternée, caractérisé en ce que cette réinversion est effectuée par une démodulation synchrone du signal au spectre alternativement inversé, séparé de l'autre porteuse par un filtrage passe-bas, au moyen d'une onde localement élaborée, synchronisée avec l'autre porteuse dont le prélèvement est effecuté au moyen d'un filtrage passe-bande.

7. Procédé de transmission cryptée suivant les revendications 5 et 6, caractérisé en ce que la suite pseudo-aléatoire ou le signal lui correspondant est obtenu par la démodulation d'amplitude de l'autre porteuse et elle est restituée de façon à commander l'alternance de la transmission du signal alternativement inversé et du signal réinversé, afin d'obtenir en sortie le signal somme ou préaccentué au spectre normal.

8. Procédé de transmission cryptée suivant la revendication 7, caractérisé en ce que le signal somme est soumis à un filtrage passe-bas pour en éliminer le signal de brouillage et en ce que le signal préaccentué est soumis à une désaccentuation de façon à atténuer la transmission des composantes de son spectre aux fréquences élevées, de manière inverse à la préaccentuation.

9. Procédé de transmission cryptée suivant la revendication 8, caractérisé en ce que le filtrage passe-bas éliminant le signal de brouillage et la désaccentuation sont effectués de manière combinée au moyen d'un filtrage complexe.

10. Procédé de transmission cryptée suivant l'une des revendications précédentes, caractérisé en ce que, à l'encryptage, la suite pseudo-aléatoiree commandant l'alternance de la transmission du signal préaccentué, éventuellement brouillé, avec des spectres respectivement normal et inversé, est transcodée de manière prédéterminée avant sa transmission par la modulation de l'autre porteuse ou par d'autres moyens, et en ce que, au décryptage, le signal transcodé ainsi obtenu est décodé de façon prédéterminé, afin de

restituer, au moins approximativement, la suite pseudo-aléatoire initiale.

11. Procédé de transmission cryptée d'un signal, notamment d'un signal audio-fréquence, comprenant une partie d'encryptage destiné à transformer de manière prédéterminée un signal clair en un signal inintelligible et une partie de décryptage destiné à retransformer ce dernier par des opérations adaptées au cryptage, en un signal clair restitué, caractérisé en ce que le procédé d'encryptage comprend en combinaison : une préaccentuation du signal clair afin d'accroître l'énergie de ses composantes de fréquences élevées de manière croissante en fonction de celle-ci ; un prélèvement par filtrage passe-bas de la partie basse-fréquence du signal préaccentué ; une transposition au moyen d'une première porteuse localement engendrée, de cette partie basse-fréquence à une fréquence supérieure à la fréquence maximale du signal préaccentué ; l'addition à ce dernier de sa partie basse-fréquence transposée qui constitue alors un signal de brouillage rendant le signal somme résultant de l'addition sensiblement inintelligible, l'élaboration d'un signal somme au spectre inversé par la modulation d'amplitude d'une seconde porteuse également localement élaborée, dont la fréquence est supérieure à la fréquence maximale du signal somme ; la transmission alternée, commandée par une suite pseudo-aléatoire élaborée localement de manière connue en soi, de telle sorte que l'on obtient en sortie un signal comprenant le signal somme transmis alternativement avec un spectre normal et un spectre inversé ; la transmission par la modulation d'une troisième porteuse d'élaboration locale, dont la fréquence est égale à celle de la seconde porteuse ou à un multiple entier de cette dernière qui est, dans ce dernier cas, obtenue par une division de fréquence à partir de la troisième, et supérieure à la fréquence maximale des spectres normal et/ou inversé du signal somme, et qui est modulée par un signal correspondant à cette suite pseudo-aléatoire ; et l'addition de la troisième porteuse modulée au signal somme au spectre alternativement inversé.

12. Procédé de transmission cryptée suivant la revendication 11, caractérisé en ce que le procédé de décryptage comprend en combinaison : une séparation du signal somme au spectre alternativement inversé au moyen d'un filtrage passe-bas et de la troisième porteuse modulée au moyen d'un filtrage passe-bande ; l'élaboration à partir de la troisième porteuse séparée, d'une onde locale asservie en fréquence et en phase à celle-ci, l'élaboration à partir de cette onde locale d'une onde de démodulation ayant une fréquence égale à celle de la seconde porteuse, éventuellement par une division de fréquence analogue à celle effectuée à l'encryptage ; la réinversion du spectre du signal somme au spectre alternativement inversé au moyen d'une démodulation synchrone à l'aide de l'onde de démodulation ; la démodulation de la troisième porteuse modulée afin de restituer le signal correspondant à la suite pseudo-aléatoire qui la module et l'élaboration de cette dernière de manière connue en soi ; l'utilisation de la suite pseudo-aléatoire pour commander le prélèvement alterné par commutation du signal somme alternativement inversé après le filtrage passe-bas et après la réinversion par démodulation synchrone, en synchronisme avec l'alternance à l'encryptage ; un autre filtrage passe-bas du signal ainsi commuté afin d'en éliminer le signal de brouillage et une désaccentuation qui est une opération inverse à la préaccentuation, du signal préaccentué ainsi obtenu, les deux dernières opérations pouvant être combinées dans un même filtre.

13. Procédé de transmission cryptée suivant l'une quelconque des revendications 11 et 12, caractérisé en ce que les écarts de fréquence entre la fréquence maximale du spectre du signal préaccentué et la fréquence minimale de celui du signal de brouillage transposé est choisie sensiblement égale à la fréquence minimale du premier.

14. Procédé de transmission cryptée suivant l'une quelconque des revendications 11 à 13, caractérisé en ce que le signal correspondant à la suite pseudo-aléatoire est obtenu au moyen d'un transcodage (numérique) de celle-ci et en ce qu'un décodage au

décryptage le transforme en une suite pseudo-aléatoire sensiblement identique et synchrone avec celle engendrée à l'encryptage.

15. Procédé de transmission cryptée suivant l'une quelconque des revendications 11 à 14, caractérisé en ce que les fréquences maximales et minimales respectives des spectres des signaux somme normal et inversé sont sensiblement les mêmes, c'est-à-dire qu'ils occupent sensiblement la même bande de fréquences.

16. Procédé de transmission cryptée suivant l'une quelconque des revendications 11 à 15, caractérisé en ce que la fréquence de la troisième porteuse destinée à être transmise modulée par le signal correspondant à la suite pseudo-aléatoire est la double de celle de la seconde qui est utilisée pour l'inversion à l'encryptage et la réinversion au décryptage, du spectre du signal somme.

17. Procédé de transmission cryptée suivant l'une quelconque des revendications 11 à 15, caractérisé en ce que la fréquence de la troisième porteuse est égale à celle de la seconde, le signal correspondant à la suite pseudo-aléatoire étant transmis au moyen d'une bande latérale unique de modulation qui est la supérieure, sa démodulation au décryptage étant alors effectuée de manière synchrone.

18. Système de transmission cryptée d'un signal, notamment d'un signal audio-fréquence, fournie par une source (1), et comprenant un dispositif d'encryptage (10) transformant le signal clair en un signal inintelligible afin de le transmettre ou diffuser uniquement à un auditoire autorisé, et un dispositif de décryptage (30) transformant le signal encrypté en un signal intelligible, correspondant sensiblement à celui fourni par la source, caractérisé en ce que le dispositif d'encryptage (10) comporte : un dispositif de préaccentuation (2) du signal clair (SC) dont le gain augmente avec la fréquence ; un générateur (4, 5, 6, 7, 8) d'un signal de brouillage (SBT) dont la fréquence minimale est supérieure à la fréquence maximale du signal préaccentué (SP) ; un étage additionneur analogique (3) fournissant un signal (SP + SBT) constituant la somme des signaux préaccentué (SP) et de brouillage (SBT) ; un générateur de

porteuse (7, 12, 13) fournissant une onde d'une fréquence supérieure à la fréquence maximale du signal somme (SP + SBT) ; un modulateur d'amplitude (11) recevant, d'une part, ce dernier et d'autre part, l'onde du générateur (7, 12, 13) pour engendrer une bande latérale inférieure contenant le signal somme avec le spectre inversé (SBI + SPI) ; un filtre passe-bas (14) séparant cette bande latérale inférieure de la porteuse et des autres produits de modulation qu'il élimine ; un générateur de suite pseudo-aléatoire (7, 16) fournissant un signal binaire (SPA) dont les deux états alternants présentent respectivement des durées variables de manière aléatoire, connu en soi ; un premier commutateur (9) dont une entrée de signal (90) reçoit le signal somme normal (SP + SBT), dont l'autre entrée de signal (91) reçoit celui avec le spectre inversé (SBI + SPI) et dont l'entrée de commande reçoit la suite pseudo-aléatoire (SPA), afin que sa sortie (92) fournisse le signal somme avec les spectres alternativement inversés ; un signal correspondant à la suite pseudo-aléatoire (SPA) étant éventuellement transmise par une modulation de la porteuse ou d'une porteuse supplémentaire dont la fréquence est un multiple entier de celle de la précédente. (figure 12)

19. Système suivant la revendication 18, caractérisé en ce que le générateur (4-8) du signal de brouillage (SBT) comprend en cascade un autre filtre passe-bas (4) recevant le signal préaccentué (SP) afin d'en transmettre la partie basse-fréquence du spectre (SB) ; un autre générateur de porteuse (7, 6) engendrant une autre onde dont la fréquence est égale ou supérieure à la fréquence maximale des signaux clair (SC) et préaccentué (SP) ; un autre modulateur d'amplitude (5) recevant, d'une part, cette partie basse-fréquence (SB) et d'autre part, l'autre onde, afin que la bande latérale supérieure de modulation de celle-ci soit située au-dessus du spectre du signal préaccentué (SP) ; et un filtre passe-bande (8) permettant la transmission de cette bande latérale supérieure (BLS) contenant la partie basse-fréquence (SB) transposée (SBT) vers le haut, qui constitue alors le signal de brouillage. (figure 12)

20. Système de transmission suivant l'une quelconque des revendications 18 et 19, caractérisé en ce que le dispositf de décryptage (30) comporte un filtre passe-bas d'entrée (22) pour transmettre uniquement le signal somme au spectre alternativement inversé ; un filtre passe-bande d'entrée (23) séparant la porteuse ou la porteuse supplémentaire, éventuellement modulée, du reste du signal et alimentant une boucle à verrouillage de phase (26) pour engendrer une onde locale à fréquence et phase asservies et pour fournir une onde de démodulation asservie à la porteuse ; un démodulateur synchrone (25) alimenté, d'une part, par le filtre passe-bas d'entrée (22) et d'autre part, par l'onde de démodulation, pour obtenir la réinversion du spectre du signal somme au spectre inversé (SBI + SPI), lorsqu'il est transmis ; un second commutateur (24) dont la première entrée de signal (240) est reliée à la sortie du filtre passe-bas d'entrée (22), dont la seconde entrée de signal (241) est couplée à la sortie du démodulateur synchrone (25) et dont l'entrée de commande (243) est alimenté par la suite pseudo-aléatoire (SPA) transmise par ailleurs ou reconstituée par démodulation de la porteuse ou de la porteuse supplémentaire reçue, éventuellement après transcodage ; la sortie (242) du second commutateur (24) fournissant alors alternativement le signal somme normal (SP + SBT) et le signal somme au spectre inversé (SBI + SPI) après sa réinversion, à un dispositif de filtrage passe-bas de sortie (31) éliminant le signal de brouillage (SBT) et à un dispositif de désaccentuation (32) ayant une fonction de transfert inverse de celui de préaccentuation (2), ces deux derniers dispositifs pouvant être combinés en un dispositif unique, afin de restituer un signal sensiblement identique à celui fourni par la source (1). (figure 13)

FIG_1

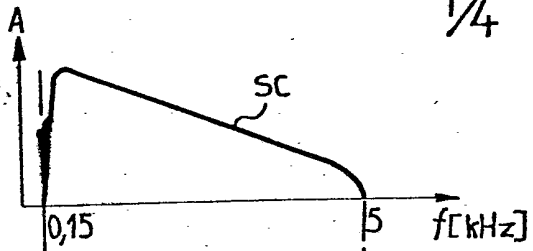


FIG_2

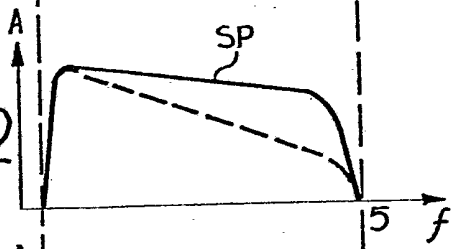


FIG_3

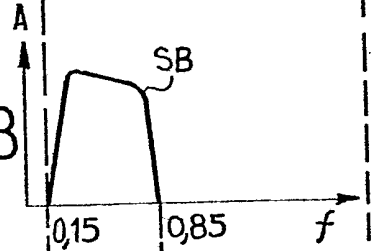


FIG_4

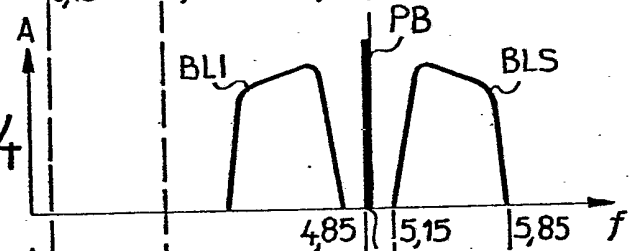


FIG_5

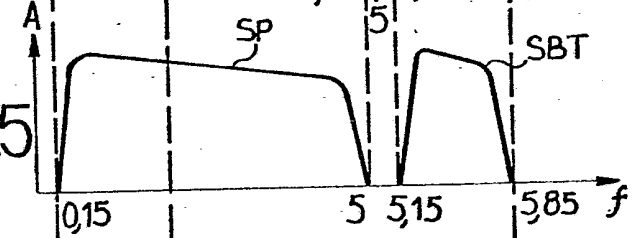


FIG_6

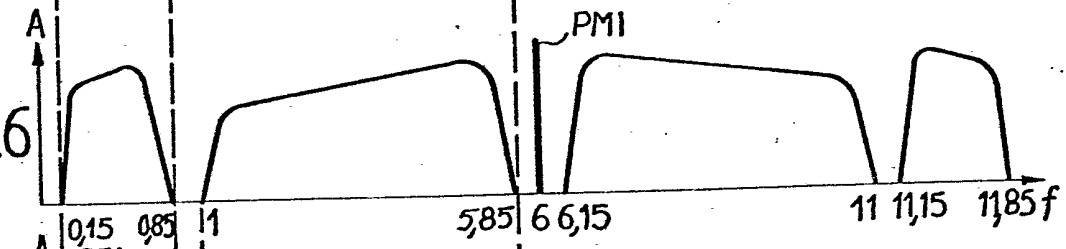


FIG_7

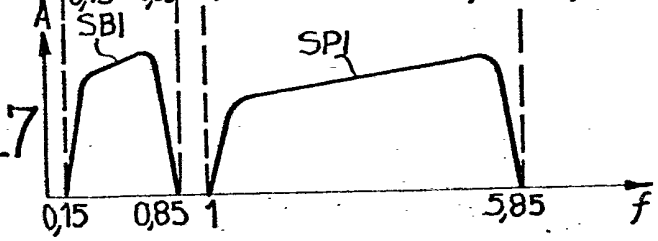


FIG_8

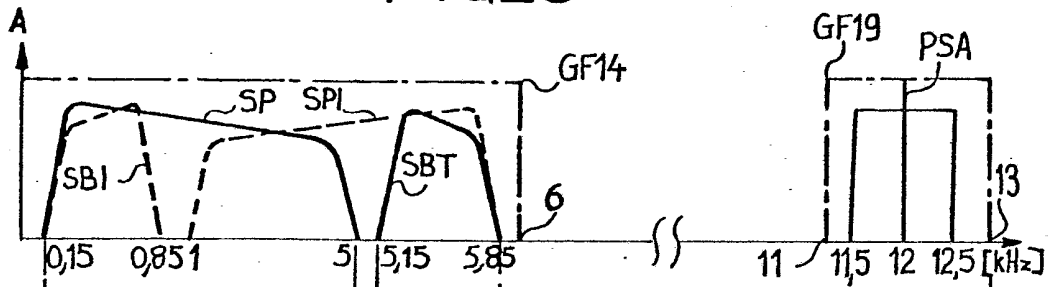


FIG_9

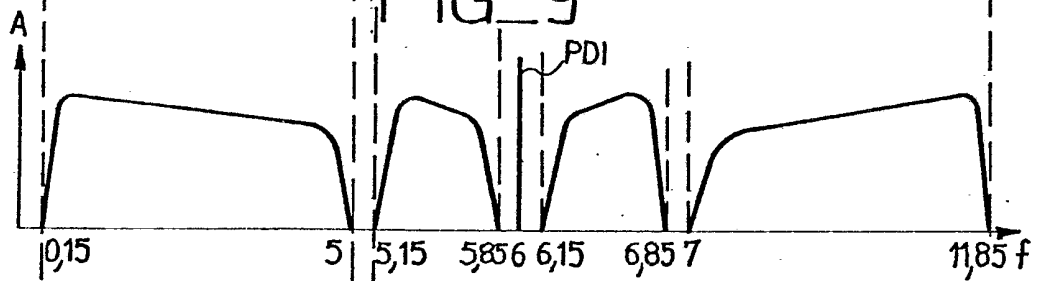


FIG_10

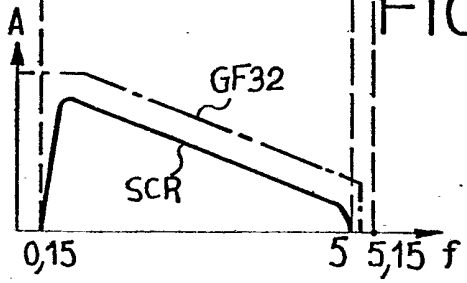


FIG_11

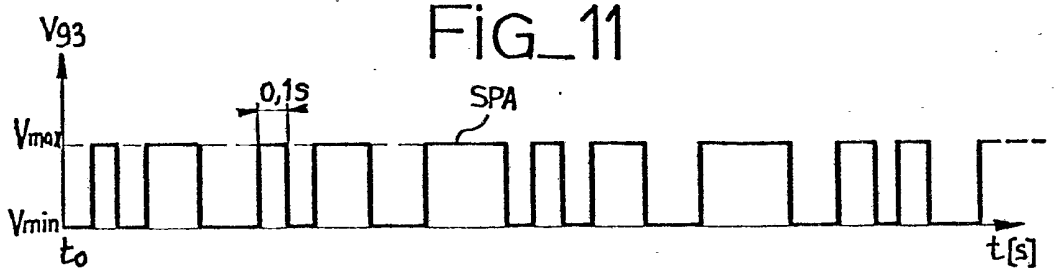


FIG_12

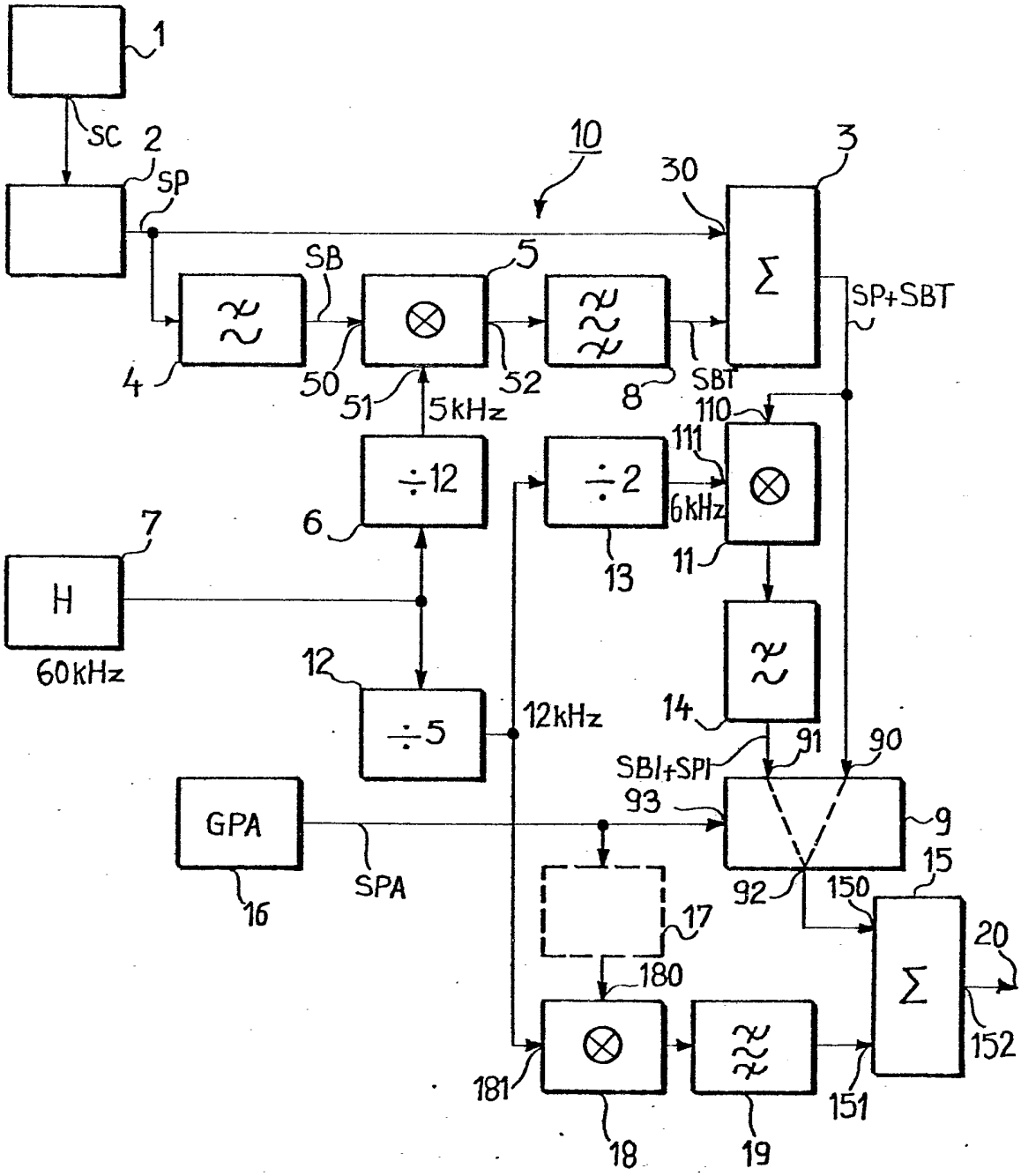
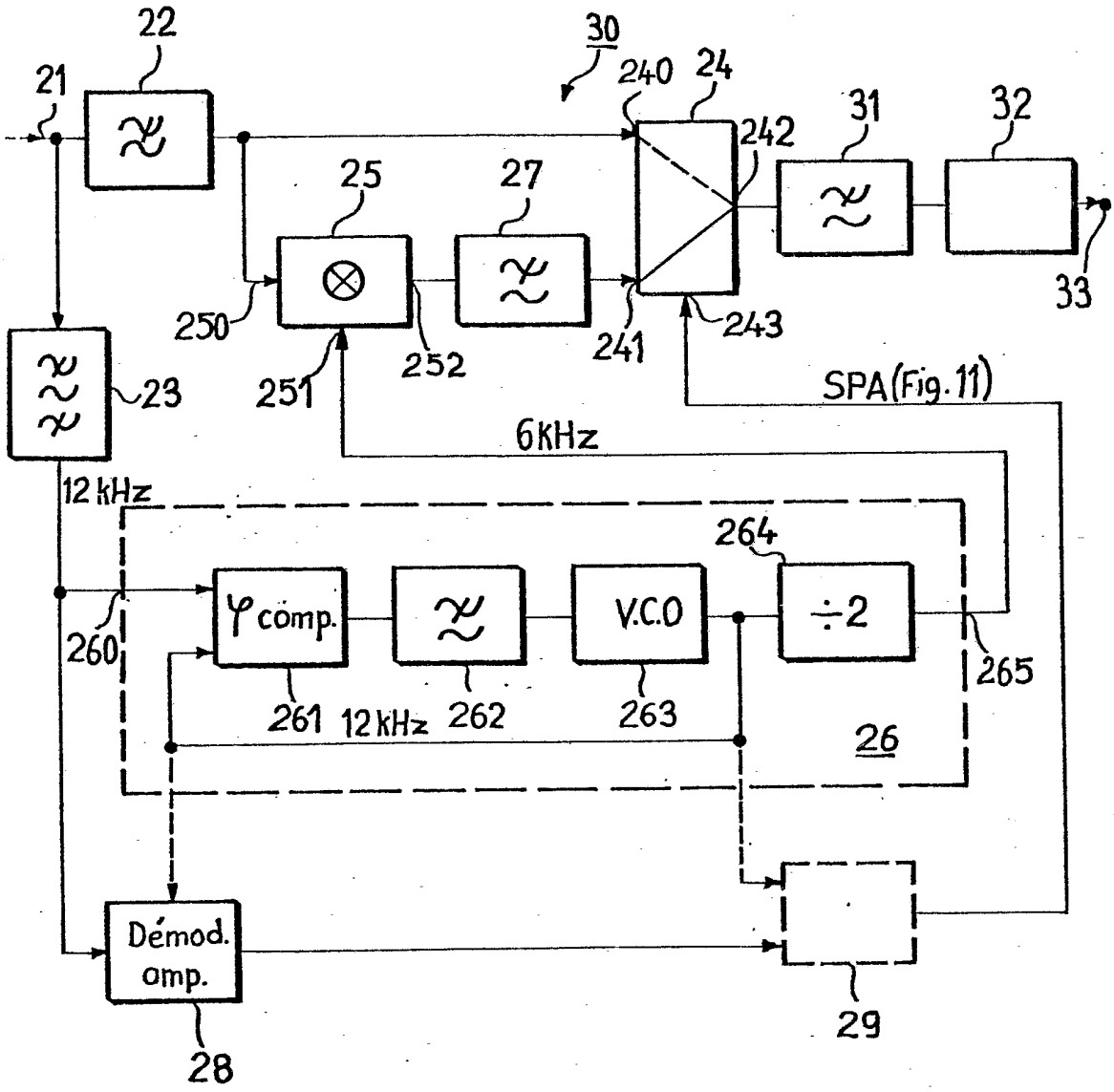

1
SC
2
SP
10
30
3
Σ
SP+SBT
SB
5
4
50
51
52
8
SBT
5kHz
÷12
6
÷2
6kHz
111
110
11
13
7
H
60kHz
12
÷5
12kHz
14
91
90
SBI+SPI
93
9
GPA
SPA
16
92
150
15
17
180
20
152
181
18
19
151

FIG_13


22
21
30
240
24
242
31
32
25
27
250
252
241
243
33
23
251
SPA(Fig.11)
6KHz
12 kHz
264
260
φ comp.
V.C.O
÷2
265
261
12 kHz
262
263
26
Démod.
amp.
29
28