(19) RÉPUBLIQUE FRANÇAISE

INSTITUT NATIONAL
DE LA PROPRIÉTÉ INDUSTRIELLE

PARIS

(11) N° de publication : **2 575 891**
(à n'utiliser que pour les commandes de reproduction)

(21) N° d'enregistrement national : **85 00179**

(51) Int Cl⁴ : H 04 N 7/267.

(12) DEMANDE DE BREVET D'INVENTION A1

(22) Date de dépôt : 8 janvier 1985.

(30) Priorité :

(43) Date de la mise à disposition du public de la demande : BOPI « Brevets » n° 28 du 11 juillet 1986.

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

(71) Demandeur(s) : *LABORATOIRES D'ELECTRONIQUE ET DE PHYSIQUE APPLIQUEE, LEP, société anonyme.* — FR.

(72) Inventeur(s) : Gérard Marie et Jean-Pierre Arragon.

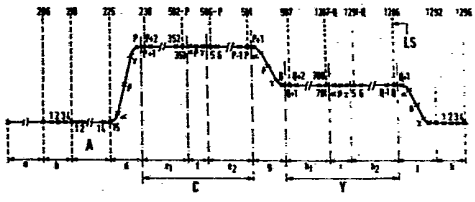
(73) Titulaire(s) :

(74) Mandataire(s) : Christian Landousy.

(54) Dispositif de décodage et de déchiffrement de signaux ayant subi un codage de type MAC et un chiffrement par permutation circulaire autour d'un ou de deux points de coupure, et dispositif de codage et de chiffrement fonctionnant de façon similaire.

(57) Dispositif de décodage et de déchiffrement de signaux ayant subi un codage de type MAC et un chiffrement par permutation circulaire à un point de coupure, c'est-à-dire par permutation circulaire de l'ensemble des signaux de chrominance C et de luminance Y à partir d'une abscisse a située dans le signal de chrominance en utilisant une fréquence d'échantillonnage f_o, ou à deux points de coupure, c'est-à-dire par permutation circulaire indépendante des signaux de chrominance C et de luminance Y à partir d'abscisses respectives a_c et a_y en utilisant une fréquence d'échantillonnage f_o, caractérisé notamment en ce que l'on utilise à la réception une fréquence d'échantillonnage f_r différente de f_o et reliée à cette dernière par la relation $f_r = q/p\ f_o$, p et q étant entiers, et en ce que la ou les nouvelles adresses de points de coupure sont prises égales la première à la valeur entière la plus proche du résultat a' de l'opération $a' = p/q\ a$ et les secondes aux valeurs entières les plus proches des résultats a'_c et a'_y des opérations $a'_c = p/q\ a_c$ et $a'_y = p/q\ a_y$.

Application aux récepteurs de télévision au standard MAC.



FR 2 575 891 - A1

DISPOSITIF DE DECODAGE ET DE DECHIFFREMENT DE SIGNAUX AYANT SUBI UN CODAGE DE TYPE MAC ET UN CHIFFREMENT PAR PERMUTATION CIRCULAIRE AUTOUR D'UN OU DE DEUX POINTS DE COUPURE, ET DISPOSITIF DE CODAGE ET DE CHIFFREMENT FONCTIONNANT DE FAÇON SIMILAIRE

La présente invention concerne un dispositif de décodage et de déchiffrement de signaux ayant subi d'une part un codage de type MAC et d'autre part un chiffrement par permutation circulaire.

Le codage de signaux vidéo selon le standard MAC (Multiplex Analogique de Composantes) consiste à assurer, pour chacune des lignes de l'image, la transmission successive des composantes analogiques de chrominance et de luminance. Le chiffrement par permutation circulaire consiste à couper, à l'émission, le signal d'image en un point quelconque et à permuter les deux fragments de ligne utiles ainsi formés, la permutation circulaire inverse étant bien entendu effectuée à la réception pour restituer en clair le signal d'image ainsi brouillé. Ce chiffrement est à un point de coupure lorsqu'une seule des deux composantes de chrominance ou de luminance est fractionnée en deux signaux, ou à deux points de coupure lorsque chacune des deux composantes subit ladite permutation circulaire autour d'un point de coupure qui lui est propre.

Le problème qui se pose est celui de l'échantillonnage, à des fréquences différentes à l'émission et à la réception, de signaux de type MAC ayant subi à l'émission un chiffrement. Ce problème peut se rencontrer en effet lorsque l'on voudra émettre des signaux de télévision codés selon un standard MAC, par exemple, avec un format d'image plus grand que le format 4/3 et/ou avec une résolution plus grande que celle des émissions précédentes, et que l'on voudra que ces émissions soient reçues de façon compatible par les récepteurs de première génération adaptés à un format d'image plus réduit (4/3) et/ou à une résolution plus faible.

Pour donner des exemples concrets, on peut se

placer dans le cas où les émissions de première génération correspondent au standard MAC défini dans la publication SPB 284 3e version révisée (décembre 1984) de l'UER (Union Européenne de Radiodiffusion). Avant codage MAC et chiffrement, les signaux sont échantillonnés à raison d'environ 700 points pour la luminance (fréquence d'échantillonnage 13,5 MHz) et de 350 points pour la chrominance (fréquence d'échantillonnage 6,75 MHz). Lorsque ces signaux sont codés en MAC en utilisant un rapport des taux de compression chrominance à luminance $r = \frac{C_c}{C_y} = 2$, la fréquence d'échantillonnage f_o en sortie du codeur chiffreur est de 20,25 MHz. Le chiffrement est réalisé par permutation circulaire effectuée soit sur les signaux de luminance Y et de chrominance C pris séparément, soit sur l'ensemble des signaux Y et C, ces signaux subissant des décalages temporels multiples d'un intervalle de base $\tau_o = 1/f_o \sim 49$ ns.

Dans le but d'augmenter la résolution luminance, on peut envisager dans le futur de choisir un rapport r des taux de compression égal à 4 au lieu de 2. Ceci est déjà possible lorsque les signaux sont transmis en modulation d'amplitude sur des réseaux câblés par exemple. Ce sera également possible dans le futur pour les transmissions par satellites en modulation de fréquence lorsque la sensibilité des récepteurs aura été améliorée et qu'ils pourront restituer, avec un rapport signal sur bruit convenable, des signaux qui auront subi des compressions temporelles d'un facteur 5 au lieu du facteur 3 actuel. Avec ce rapport r = 4, si la fréquence d'échantillonnage et l'intervalle de base utilisés pour le chiffrement restent inchangés, le signal de luminance comportera environ 840 intervalles au lieu de 700. Pour effectuer le déchiffrement à partir du même intervalle de base qu'à l'émission, il faudrait disposer dans le récepteur de mémoires de luminance de 840 échantillons au lieu de 700, ce qui n'est pas prévu dans les récepteurs de première génération construits avec des mémoires de 700 échantillons seulement et rend cette

solution incompatible avec ces récepteurs.

Pour pouvoir se contenter de mémoires de luminance de 700 échantillons, on peut alors songer à réduire la fréquence d'échantillonnage à la réception à la valeur $f_r = \frac{5}{6} f_o = 16{,}875$ MHz. Il faut alors modifier les adresses a des points de coupure (données par un générateur d'adresses pseudo-aléatoires) en calculant les nouvelles adresses $a' = \frac{5}{6} a$. Comme, à l'émission, il y a, par exemple dans le signal de luminance, 256 adresses possibles séparées par des intervalles égaux à $2\tau_o$, la nouvelle adresse a' correspondra deux fois sur trois à une valeur non entière. Dans le cas du signal de chrominance, pour lequel les adresses sont séparées par un intervalle égal à τ_o, c'est cinq fois sur six que l'adresse a' ne sera pas entière. Comme on ne met en mémoire qu'un nombre discret d'échantillons (700 pour Y, 175 pour C), l'adresse réelle utilisée sera la valeur entière de a' la plus proche de sa valeur théorique et l'on fera donc une erreur sur la référence temporelle de chaque ligne qui pourra atteindre un demi-intervalle d'échantillonnage à la réception. Une ligne verticale de l'image sera donc restituée en fait comme une ligne légèrement en zig-zag, l'amplitude crête à crête de ce zig-zag atteignant environ la largeur d'un espace d'échantillonnage, c'est-à-dire 1/700e de la largeur d'image dans le cas de la chrominance et 1/175e dans celui de la luminance.

Lorsqu'on engendre la fréquence $f_r = \frac{5}{6} f_o$, la division par 6 donne six possibilités de phase pour la fréquence f_r. Il y a donc six signaux d'échantillonnage possibles f_{r_o},, f_{r_1},... f_{r_5} qui diffèrent l'un de l'autre d'un écart de phase égal à $\pi/3$. Si l'on passe du signal f_{r_i} au signal $f_{r_{i+1}}$, on avance de $\pi/3$ la phase de la fréquence d'échantillonnage, ce qui revient à avancer d'une valeur égale à $\tau_r/6$ les instants d'échantillonnage. Lors de la lecture de la mémoire, cela se traduira sur l'image par un décalage vers la droite de la ligne correspondante d'une distance égale à $\frac{1}{6} \times \frac{1}{700}$ de la largeur d'image.

Un premier but de l'invention est de proposer un dispositif de décodage et de déchiffrement de signaux de type MAC chiffrés par permutation circulaire dans lequel on corrige le défaut introduit par le changement de la fréquence d'échantillonnage de réception en profitant de cette possibilité de décaler les lignes restituées.

Le dispositif selon l'invention est à cet effet, dans le cas d'un chiffrement à deux points de coupure, caractérisé en ce que l'on utilise à la réception une fréquence d'échantillonnage f_r différente de f_o et reliée à cette dernière par la relation $f_r = \frac{q}{p} f_o$, p et q étant entiers, en ce que les nouvelles adresses de points de coupure sont prises égales aux valeurs entières les plus proches des résultats a'_c et a'_y des opérations $a'_c = \frac{p}{q} a_c$ et $a'_y = \frac{p}{q} a_y$, et en ce que, au début de l'écriture en mémoire de chaque composante C ou Y, à partir de l'abscisse a'_c ou a'_y respectivement, la fréquence d'échantillonnage f_r subit soit une avance de phase qui, exprimée en période d'échantillonnage $\tau_r = 1/f_r$, est égale à la partie fractionnaire g_c ou g_y du résultat a'_c ou a'_y lorsque g_c ou g_y est inférieure à 1/2, ou respectivement inférieure ou égale à 1/2, soit un retard de phase égal à $1 - g_c$ ou $1 - g_y$ lorsque g_c ou g_y est supérieure ou égale à 1/2, ou respectivement supérieure à 1/2.

Dans le cas d'un chiffrement à un point de coupure, ce dispositif est caractérisé en ce que l'on utilise à la réception une fréquence d'échantillonnage f_r différente de f_o et reliée à cette dernière par la relation $f_r = \frac{p}{q} f_o$, p et q étant entiers, en ce que la nouvelle adresse du point de coupure est prise égale à la valeur entière la plus proche du résultat a' de l'opération $a' = \frac{p}{q} a$, et en ce que, au début de l'écriture en mémoire de la composante C à partir de l'abscisse a', la fréquence d'échantillonnage f_r subit soit une avance de phase qui, exprimée en période d'échantillonnage $\tau_r = 1/f_r$, est égale à la partie fractionnaire g du résultat a' lorsque g est inférieure à 1/2, ou respectivement inférieure ou égale à 1/2, soit un retard de phase égal à 1 - g

lorsque g est supérieure ou égale à 1/2, ou respectivement supérieure à 1/2.

La structure ainsi proposée est avantageuse en ce sens qu'on profite effectivement de la possibilité de décalage des lignes restituées en faisant commander le choix de la phase de la fréquence f_r par la valeur g de la partie fractionnaire du résultat de l'opération a' = 5a/6.

En effet, suivant que cette valeur est égale à 0, $\frac{1}{6}$, $\frac{2}{6}$... $\frac{5}{6}$, on choisira la fréquence f_{r_0}, f_{r_1}, ... f_{r_5}, c'est à-dire que l'on introduira une avance égale à 0, $\frac{1}{6}\tau_r$ ... $\frac{5}{6}$ τ_r ce qui permettra de faire coïncider sur deux verticales le début et la fin de chaque ligne. Cela revient à avancer l'instant d'échantillonnage du premier échantillon reçu vers l'échantillon répété (overlap), ce qui n'occasionne pas de discontinuité dans le signal si les références temporelles de la synchronisation et de la vidéo sont bien respectées. Afin de laisser une certaine tolérance sur cette référence temporelle, il est préférable de répartir les décalages en avance et en retard en choisissant de faire subir à la fréquence f_o soit une avance de phase qui, exprimée en période τ_r, est égale à g lorsque g est inférieure (inférieure ou égale) à 1/2, soit un retard de phase égal à 1 - g lorsque g est supérieure ou égale (supérieure) à 1/2. L'adresse du point de coupure à prendre en compte est alors la valeur entière immédiatement inférieure à a', lorsque g est inférieure (inférieure ou égale) à 1/2, et immédiatement supérieure à a', lorsque g est supérieure ou égale (supérieure) à 1/2.

La correction du défaut ne sera cependant pas totale lorsque la longueur de la ligne restituée ne sera pas égale à la longueur originelle, ce qui est le cas lorsque, à la fréquence f_r, il n'y a pas un nombre entier d'intervalles d'échantillonnage entre le premier échantillon utile reçu et l'échantillon répété (overlap) qui suit le dernier échantillon utile reçu.

L'invention y remédie par une quatrième mesure, le

dispositif étant alors caractérisé en outre en ce que, dans le cas du chiffrement à deux points de coupure, lorsque l'on atteint l'adresse maximale en mémoire de chrominance ou de luminance, l'on recommence l'écriture des échantillons au début de la mémoire de chrominance ou de luminance après avoir marqué un temps d'arrêt correspondant à quelques échantillons de transition et après avoir fait subir à la fréquence d'échantillonnage f_r un retard de phase qui, exprimé en période d'échantillonnage $\tau_r = 1/f_r$, est égal à la partie fractionnaire h_c ou h_y du résultat δ'_c ou δ'_y de l'opération $\delta'_c = \frac{p}{q} \delta_c$ ou $\delta'_y = \frac{p}{q}\delta_y$, δ_c étant égal au nombre d'intervalles d'échantillonnage, à la fréquence f_o, qui séparent le premier échantillon C utile émis de l'échantillon répété qui suit le dernier échantillon C utile émis et δ_y étant égal au nombre d'intervalles d'échantillonnage, à la fréquence f_o, qui séparent le premier échantillon Y utile émis de l'échantillon répété qui suit le dernier échantillon Y utile émis.

Dans le cas du chiffrement à un point de coupure, cette quatrième mesure est telle que le dispositif est caractérisé en ce que, en plus des temps d'arrêt qui correspondent à quelques échantillons de transition et que l'on marque quand on passe de l'écriture dans la mémoire de chrominance à celle dans la mémoire de luminance puis de l'écriture dans la mémoire de luminance de nouveau à celle dans la mémoire de chrominance, l'on fait subir à la fréquence d'échantillonnage f_r, après le premier temps d'arrêt, un retard de phase qui, exprimé en période τ_r, est égal à la partie fractionnaire h_c du résultat δ'_c de l'opération $\delta'_c = \frac{p}{q} \delta_c$, δ_c étant égal au nombre d'intervalles d'échantillonnage, à la fréquence f_o, correspondant à la somme du signal C et de la première transition, et, après le second temps d'arrêt, un retard de phase égal à la partie fractionnaire h_y du résultat δ'_y de l'opération $\delta'_y = \frac{p}{q} \delta_y$, δ_y étant égal au nombre d'intervalles d'échantillonnage, à la fréquence f_o, correspondant à la somme du signal Y et de la seconde transition.

Un autre but de l'invention est de proposer à l'émission un dispositif de codage et de chiffrement pour émetteur de signaux de télévision selon le standard MAC, destiné à coopérer aussi bien avec un récepteur conventionnel qu'avec un récepteur comprenant l'un des dispositifs de décodage et de déchiffrement selon la présente invention, et comprenant à cet effet des circuits similaires à ceux de l'un de ces dispositifs de façon à réduire la vitesse des circuits de traitement et la capacité des mémoires nécessaires.

Les particularités et avantages de l'invention apparaîtront maintenant de façon plus précise dans la suite de la description et dans les figures 1 et 2 qui illustrent les propositions de codage et chiffrement de l'UER de décembre 1984 dans le cas d'un chiffrement respectivement à deux points de coupure et à un seul point de coupure situé dans le signal de chrominance.

Sur la figure 1, qui montre la forme d'onde du signal de modulation à l'émission dans le cas du chiffrement à deux points de coupure, on a désigné par A l'intervalle d'alignement du signal, C la durée du signal de chrominance, Y celle du signal de luminance et LS le dernier échantillon à mémoriser. Le nombre d'intervalles, à la fréquence d'échantillonnage f_o = 20,25 MHz, que l'on doit considérer est égal à :

(a)
- 352 intervalles C, soit 349 échantillons utiles et 3 transitions
- 700 intervalles Y, soit 697 échantillons utiles et 3 transitions.

En choisissant un rapport des taux de compression $r = C_c/C_y = 4$, on peut avoir soit :

(b)
- 212 intervalles C, soit 209 échantillons utiles et 3 transitions
- 840 intervalles Y, soit 837 échantillons utiles et 3 transitions

soit :

(c) $\begin{cases} 213 \text{ intervalles C, soit 210 échantillons utiles et} \\ 3 \text{ transitions} \\ 839 \text{ intervalles Y, soit 836 échantillons utiles et} \\ 3 \text{ transitions} \end{cases}$

En choisissant une fréquence d'échantillonnage à la réception $f_r = \frac{5}{6} f_o$, le nombre d'intervalles devient $\delta' = \frac{5}{6}$ soit :

dans le cas (b) $\begin{matrix} 176\ \frac{2}{3} \\ 700 \end{matrix}$ intervalles $\begin{matrix} C \\ Y \end{matrix}$

dans le cas (c) $\begin{matrix} 177\ \frac{1}{2} \\ 699\ \frac{1}{6} \end{matrix}$ " $\begin{matrix} C \\ Y \end{matrix}$

Pour que le dernier échantillon utile écrit, situé juste avant la coupure, soit géométriquement distant exactement d'un intervalle d'échantillonnage du premier échantillon utile écrit, situé juste après la coupure, il faut que ce dernier échantillon écrit soit distant temporellement exactement d'un intervalle d'échantillon τ_r de l'échantillon répété (overlap) qui le suit et qui coïncide géométriquement sur l'image avec le premier échantillon reçu. Comme tous les échantillons utiles devront être équidistants, le seul moyen de rattraper éventuellement une valeur non entière de l'intervalle d'échantillonnage total est de faire porter la partie non entière sur les intervalles de transition soit :

dans le cas (b) $\begin{cases} 176\ \frac{2}{3} \text{ intervalles C} = 174 \text{ échantillons utiles} \\ \quad + 2\frac{2}{3} \text{ transitions} \\ 700 \text{ intervalles Y} = 697 \text{ échantillons utiles} \\ \quad + 3 \text{ transitions} \end{cases}$

dans le cas (c) $\begin{cases} 177\ \frac{1}{2} \text{ intervalles C} = 175 \text{ échantillons utiles} \\ \quad + 2\frac{1}{2} \text{ transitions} \\ 699\ \frac{1}{6} \text{ intervalles Y} = 696 \text{ échantillons utiles} \\ \quad + 3\frac{1}{6} \text{ transitions} \end{cases}$

Cette modification de l'intervalle de transition peut être obtenue très simplement en changeant la phase de la fréquence f_r lorsque l'on arrive en bout de mémoire et que l'on va écrire les échantillons suivants au début de la mémoire, après avoir marqué un temps d'arrêt de quelques échantil-

lons de transition. En pratique, cela reviendra à effectuer les temps d'arrêts et les retards ou avances de phase suivants :

dans le cas (b) { pour C arrêt durant 3 échantillons et avance de $\frac{1}{3}\tau_r$; pour Y arrêt durant 3 échantillons sans retard ni avance

dans le cas (c) { pour C arrêt durant 3 échantillons et avance de $\frac{1}{2}\tau_r$; pour Y arrêt durant 3 échantillons et retard de $\frac{1}{6}\tau_r$.

On voit que l'on peut choisir ici le nombre d'échantillons de transition à la réception égal au nombre d'échantillons de transition à l'émission et introduire soit un retard de phase égal, en fraction de τ_r, à la partie fractionnaire h du résultat de l'opération $\delta' = \frac{5}{6}\delta$ lorsque h est inférieur à 1/2, soit une avance égale à 1 - h lorsque h est supérieur ou égal à 1/2.

On peut remarquer que ces sauts de phase ne présentent pas de difficulté plus importante que ceux déjà prévus en fonction de l'abscisse du point de coupure car, dans le cas du chiffrement à deux points de coupure, il était déjà nécessaire en général d'effectuer un saut de phase entre l'échantillonnage du signal de chrominance et celui du signal de luminance qui avaient subi chacun des permutations circulaires à partir d'adresses différentes.

Dans le cas d'un signal ayant subi un chiffrement par permutation circulaire à un seul point de coupure situé dans le signal chrominance, le nombre d'intervalles d'échantillonnage entre le premier échantillon C utile et l'échantillon répété qui suit le dernier échantillon C utile comprend, comme on peut le voir sur la figure 2 qui illustre (de façon similaire au cas de la figure 1) les propositions de l'UER de décembre 1984 :

349 échantillons de chrominance séparés en 2 parties C_1 et C_2

697 échantillons de luminance

2 X 5 échantillons de transition C_2-Y et Y-C_1;

soit en tout 1 056 intervalles.

En choisissant un rapport des taux de compression $r = C_c/C_y = 4$ on peut, par exemple, répartir ces intervalles comme suit :

215 intervalles, soit 210 échantillons C utiles et 5 transitions

841 intervalles, soit 836 échantillons Y utiles et 5 transitions

En choisissant une fréquence d'échantillonnage à la réception $f_r = \frac{5}{6} f_o$, ces nombres d'intervalles deviennent respectivement $179\frac{1}{6}$ et $700\frac{5}{6}$ qui peuvent être répartis, par exemple, comme suit :

175 échantillons C suivis de $4\frac{1}{6}$ transitions

696 échantillons Y suivis de $4\frac{5}{6}$ transitions

pour que les positions du premier échantillon C en mémoire et du premier échantillon Y en mémoire, après déchiffrement, coïncident sur l'image avec les positions des premiers points C et Y utiles échantillonnés à la fréquence f_o dans le codeur.

Pour assurer le raccord correct entre les différentes parties du signal, il suffit donc de prévoir, par exemple, 4 échantillons de transition aux passages C_2-Y et Y-C_1 et de prévoir, en outre, un retard de $\frac{1}{6}\tau_r$ de la fréquence f_r à la fin de la première transition et un retard de $\frac{5}{6}\tau_r$ à la fin de la seconde.

Dans le but de simplier la réalisation du système, il est possible de réduire le nombre de phases utilisées en pratique pour f_r : on peut par exemple n'utiliser que trois phases différant l'une de l'autre de $2\pi/3$; l'erreur introduite sera égale à $\pm \frac{1}{12}\tau_r$ ce qui se traduira sur l'image par un épaississement d'un trait vertical égal à $\frac{1}{6} \times \frac{1}{700}$ de la largeur d'image en luminance, ce qui n'est certainement pas percepti-

ble. Dans le cas où l'on se contenterait de deux phases seulement différant de π, l'erreur atteindrait $\pm \frac{1}{6} \tau_r$ et l'épaississement serait de $\frac{1}{6} \times \frac{1}{700}$ de la largeur d'image en luminance, ce qui risque d'être perceptible mais pourrait sans doute être acceptable pour des récepteurs de bas de gamme. Pour la chrominance, l'épaississement serait 4 fois plus important mais ne serait vraisemblablement guère plus perceptible que celui introduit en luminance, en raison du moindre pouvoir de résolution de l'oeil vis-à-vis de la chrominance.

On peut également envisager dans l'avenir, dans le cas d'émission d'images avec un format égal à 5,33/3 par exemple, d'augmenter la résolution des images en augmentant la bande passante du signal transmis : porter par exemple à 12 GHz cette bande passante alors qu'elle est environ de 9 MHz actuellement, ce qui nécessiterait d'employer une fréquence d'échantillonnage égale au minimum à 27 MHz au lieu de la fréquence f_o = 20,25 MHz actuelle. Deux solutions peuvent être envisagées.

(A) <u>première solution</u> :

On emploie à l'émission une fréquence f_e égale à 27 MHz et l'on effectue le chiffrement à partir de cette fréquence, l'intervalle de base étant alors $\tau_e = 1/f_e \sim 37$ ns. Si le rapport r des taux de compression est égal à 2, le nombre de points échantillonnés en luminance est égal à 933 pour l'image au format 5,33/3. Le récepteur ancien devra donner une image compatible dont la largeur ne représentera que les 3/4 de celle de l'image grand format, ce qui nécessitera une capacité de mémoires de luminance de 700 échantillons égale à la capacité des mémoires que ce récepteur possède déjà.
Si, par contre, le rapport r des taux de compression a été choisi égal à 4, le nombre d'échantillons Y sera égal à 1 120 pour l'image au format élargi et 840 pour l'image au format 4/3 compatible. On se retrouve donc dans une situation identique à celle décrite précédemment ; le récepteur pourra se contenter de ses mémoires de 700 échantillons en choisissant une

fréquence d'échantillonnage égale à $\frac{5}{6} f_e = 22,5$ MHz et utilisant la même procédure que précédemment pour corriger les écarts de positionnement. Il pourrait également utiliser la fréquence de 20,25 MHz, soit $\frac{3}{4} f_e$, en prévoyant 2 ou 4 phases possibles choisies en fonction de la valeur de la partie fractionnaire du résultat de l'opération $a" = \frac{3}{4} a$, qui permet de traduire les adresses a à 27 MHz en adresse a" à 20,25 MHz, et en fonction du nombre d'intervalles d'échantillonnage entre le premier échantillon utile reçu et le dernier échantillon répété.

(B) deuxième solution :

Dans le but de simplifier les normes et pour avoir les mêmes fréquences de référence pour la vidéo et pour les données dans le multiplex temporel, il peut être avantageux de décider que toutes les émissions prendront pour base de référence de chiffrement la valeur $\tau_o = 1/f_o \sim 49$ ns. Cela n'empêche pas, à l'émission, d'étendre la bande passante du signal jusqu'à 12 MHz : il suffit pour cela par exemple d'effectuer le chiffrement en prenant comme fréquence de référence 40,5 MHz, en ne considérant que des adresses de coupure paires et en effectuant, avant émission, un filtrage pour limiter le spectre du signal émis à 12 MHz environ.

Pour la réception sur un récepteur conventionnel au format 4/3, si le rapport r des taux de compression est égal à 2, aucun problème ne se pose puisque le signal échantillonné à 20,25 MHz ne comporte que 700 échantillons de luminance. Dans le cas d'un rapport r des taux de compression égal à 4, il ne se pose pas de problème non plus car la partie 4/3 compatible du signal ne comporte que $\frac{3}{4} \times 840 = 630$ échantillons Y.

Dans le cas où l'on veut profiter pleinement de l'augmentation de la résolution à la réception, il est possible d'utiliser la même fréquence d'échantillonnage qu'à l'émission: $2 f_o = 40,5$ MHz. Il serait cependant plus économique, à la fois vis-à-vis de la rapidité des circuits et vis-à-vis de la capa-

cité des mémoires nécessaires, de se contenter d'une fréquence d'échantillonnage f_r = 27 MHz = $\frac{4}{3} f_o$. Pour corriger les erreurs de positionnement de ligne, il faudrait prévoir trois phases possibles différant de 2 $\pi/3$, pour cette fréquence, et choisir la phase utilisée en fonction de la partie fractionnaire g du résultat de l'opération $a''' = \frac{4}{3} a$ qui donne l'adresse a''' des points de coupure en fonction de l'adresse a donnée par le générateur d'adresses pseudo-aléatoires. Il faudrait en outre éventuellement, comme précédemment, changer la phase de la fréquence d'échantillonnage pour introduire, lorsque cela est nécessaire, des intervalles de transition non entiers lorsque l'on arrive en bout de mémoire et que l'on va recommencer à écrire en début de mémoire.

Si l'on se place, par exemple, dans les trois cas où le signal est émis selon les caractéristiques (a) (b) et (c) précédemment citées et avec chiffrement par permutation circulaire à deux points de coupure, l'échantillonnage à la fréquence $f_r = \frac{4}{3} f_o$ = 27 MHz va donner :

dans le cas (a) { $469\frac{1}{3}$ intervalles C soit 465 échantillons utiles et $4\frac{1}{3}$ transitions
$933\frac{1}{3}$ intervalles Y soit 929 échantillons utiles et $4\frac{1}{3}$ transitions

dans le cas (b) { $282\frac{2}{3}$ intervalles C soit 279 échantillons utiles et $3\frac{2}{3}$ transitions
1120 intervalles Y soit 1116 échantillons utiles et 4 transitions

dans le cas (c) { 284 intervalles C soit 280 échantillons utiles et 4 transitions
$1118\frac{2}{3}$ intervalles Y soit 1115 échantillons et $3\frac{2}{3}$ transitions

Avant de recommencer l'écriture des signaux en début de mémoire et après avoir marqué un temps d'arrêt de

4 échantillons de transition, il faudra en outre faire subir à la fréquence f_r :

dans le cas (a) un retard de $\frac{1}{3}\tau_r$ pour C et pour Y

dans le cas (b) une avance de $\frac{1}{3}\tau_r$ pour C

dans le cas (c) une avance de $\frac{1}{3}\tau_r$ pour Y.

Bien entendu, tous les procédés qui viennent d'être décrits dans le cas du décodage et du déchiffrement à la réception peuvent être utilisés également pour le codage et le chiffrement des signaux à l'émission où ils permettraient de réduire la vitesse des circuits de traitement et la capacité des mémoires nécessaires.

REVENDICATIONS :

1. Dispositif de décodage et de déchiffrement de signaux ayant subi un codage de type MAC et un chiffrement par permutation circulaire à deux points de coupure, c'est-à-dire par permutation circulaire indépendante des signaux de chrominance C et de luminance Y à partir d'abscisses respectives a_c et a_y en utilisant une fréquence d'échantillonnage f_o, caractérisé en ce que l'on utilise à la réception une fréquence d'échantillonnage f_r différente de f_o et reliée à cette dernière par la relation $f_r = \frac{q}{p} f_o$, p et q étant entiers, en ce que les nouvelles adresses de points de coupure sont prises égales aux valeurs entières les plus proches des résultats a'_c et a'_y des opérations $a'_c = \frac{p}{q} a_c$ et $a'_y = \frac{p}{q} a_y$ et en ce que, au début de l'écriture en mémoire de chaque composante C ou Y, à partir de l'abscisse a'_c ou a'_y respectivement, la fréquence d'échantillonnage f_r subit soit une avance de phase qui, exprimée en période d'échantillonnage $\tau_r = 1/f_r$, est égale à la partie fractionnaire g_c ou g_y du résultat a'_c ou a'_y lorsque g_c ou g_y est inférieure à 1/2, ou respectivement inférieure ou égale à 1/2, soit un retard de phase égal à $1 - g_c$ ou $1 - g_y$ lorsque g_c ou g_y est supérieure ou égale à 1/2, ou respectivement supérieure à 1/2.

2. Dispositif de décodage et de déchiffrement de signaux ayant subi un codage de type MAC et un chiffrement par permutation circulaire à un point de coupure, c'est-à-dire par permutation circulaire de l'ensemble des signaux de chrominance C et de luminance Y à partir d'une abscisse a située dans le signal de chrominance en utilisant une fréquence d'échantillonnage f_o, caractérisé en ce que l'on utilise à la réception une fréquence d'échantillonnage f_r différente de f_o et reliée à cette dernière par la relation $f_r = \frac{p}{q} f_o$, p et q étant entiers, en ce que la nouvelle adresse du point de coupure est prise égale à la valeur entière la plus proche du résultat a' de l'opération $a' = \frac{p}{q} a$ et en ce que, au début de l'écriture en mémoire de la composante C à partir de l'abscisse

a', la fréquence d'échantillonnage f_r subit soit une avance de phase qui, exprimée en période d'échantillonnage $\tau_r = 1/f_r$, est égale à la partie fractionnaire g du résultat a' lorsque g est inférieure à 1/2, ou respectivement inférieure ou égale à 1/2, soit un retard de phase égal à 1 - g lorsque g est supérieure ou égale à 1/2, ou respectivement supérieure à 1/2.

3. Dispositif selon la revendication 1, caractérisé en ce que, lorsque l'on atteint l'adresse maximale en mémoire de chrominance ou de luminance, l'on recommence l'écriture des échantillons au début de la mémoire de chrominance ou de luminance après avoir marqué un temps d'arrêt correspondant à quelques échantillons de transition et après avoir fait subir à la fréquence d'échantillonnage f_r un retard de phase qui, exprimé en période d'échantillonnage $\tau_r = 1/f_r$, est égal à la partie fractionnaire h_c ou h_y du résultat δ'_c ou δ'_y de l'opération $\delta'_c = \frac{p}{q} \delta_c$ ou $\delta'_y = \frac{p}{q} \delta_y$, δ_c étant égal au nombre d'inbre d'intervalles d'échantillonnage, à la fréquence f_o, qui séparent le premier échantillon C utile émis de l'échantillon répété qui suit le dernier échantillon C utile émis et δ_y étant égal au nombre d'intervalles d'échantillonnage, à la fréquence f_o, qui séparent le premier échantillon Y utile émis de l'échantillon répété qui suit le dernier échantillon Y utile émis.

4. Dispositif selon la revendication 2, caractérisé en ce que, en plus de temps d'arrêt qui correspondent à quelques échantillons de transition et que l'on marque quand on passe de l'écriture dans la mémoire de chrominance à celle dans la mémoire de luminance puis de l'écriture dans la mémoire de luminance de nouveau à celle dans la mémoire de chrominance, l'on fait subir à la fréquence d'échantillonnage f_r, après le premier temps d'arrêt, un retard de phase qui, exprimé en période τ_r, est égal à la partie fractionnaire h_c du résultat δ'_c de l'opération $\delta'_c = \frac{p}{q} \delta_c$, δ_c étant égal au nombre d'intervalles d'échantillonnage, à la fréquence f_o, correspondant à la somme du signal C et de la première transition,

et, après le second temps d'arrêt, un retard de phase égal à la partie fractionnaire h_y du résultat δ'_y de l'opération $\delta'_y = \frac{p}{q} \delta_y$, δ_y étant égal au nombre d'intervalles d'échantillonnage, à la fréquence f_o, correspondant à la somme du signal Y et de la seconde transition.

5. Dispositif selon l'une des revendications 1 à 4, caractérisé en ce que, p et q étant premiers entre eux et q étant divisible par 2, par 3 ou par 4, l'on n'utilise que $\frac{q}{2}$, $\frac{q}{3}$, ou $\frac{q}{4}$ états de phase de la fréquence d'échantillonnage f_r, les avances et retards considérés étant multiples de $\frac{2}{q} \tau_r$, $\frac{3}{q} \tau_r$ ou $\frac{4}{q} \tau_r$ et les avances ou retards choisis étant les plus proches des valeurs calculées à partir des parties fractionnaires des résultats des opérations $a' = \frac{p}{q} a$ et $\delta' = \frac{p}{q} \delta$.

6. Dispositif selon l'une des revendications 1 à 5, caractérisé en ce que, à la réception, le nombre d'échantillons de transition, à la fréquence f_r, est égal au nombre d'échantillons de transition, à la fréquence f_o, insérés à l'émission, multiplié par la fraction $\frac{p}{q}$ et arrondi à la valeur entière inférieure ou à la valeur entière supérieure.

7. Dispositif de codage et de chiffrement pour émetteur de signaux de télévision selon le standard MAC, destiné à coopérer avec un récepteur comprenant un dispositif de décodage et de déchiffrement selon l'une des revendications 1 à 6, et comprenant à cet effet des circuits similaires à ceux dudit dispositif de décodage de façon à réduire la vitesse des circuits de traitement et la capacité des mémoires nécessaires.

2575891

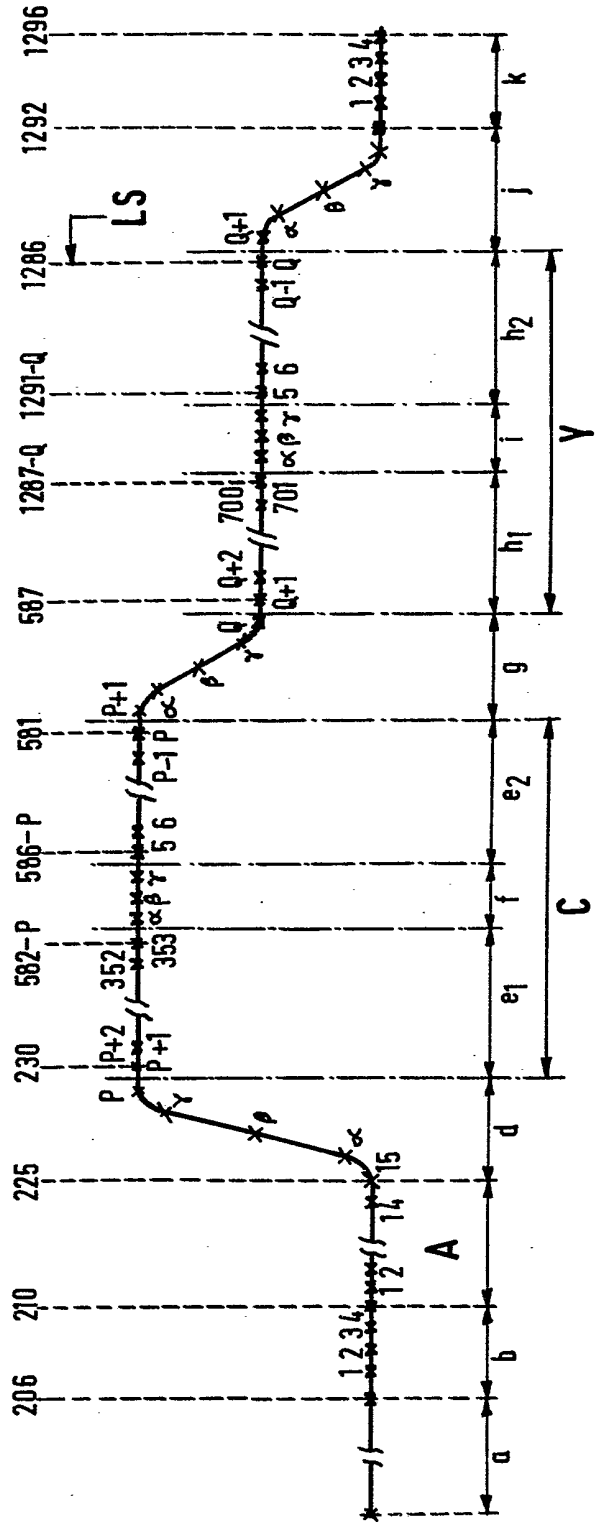


FIG.1

2575891

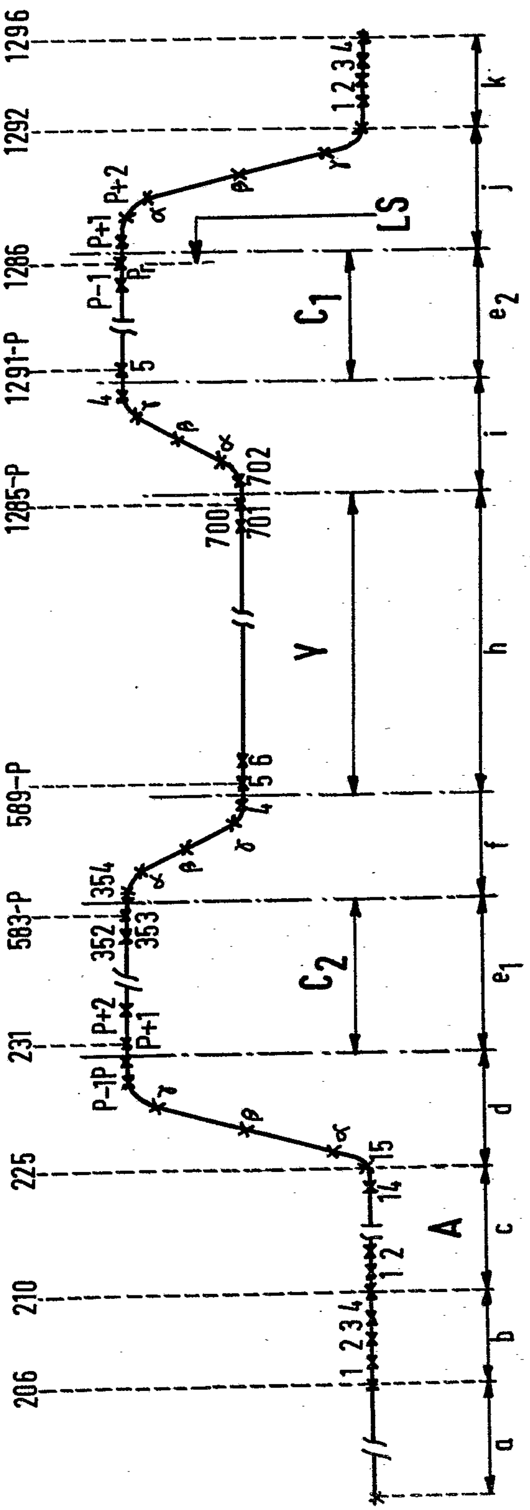


FIG.2