(19) RÉPUBLIQUE FRANÇAISE

INSTITUT NATIONAL
DE LA PROPRIÉTÉ INDUSTRIELLE

PARIS

(11) **N° de publication :** **2 806 231**
(à n'utiliser que pour les commandes de reproduction)

(21) **N° d'enregistrement national :** **00 02960**

(51) Int Cl[7] : **H 04 L 9/32,** H 04 N 1/32

(12) DEMANDE DE BREVET D'INVENTION A1

(22) **Date de dépôt :** 08.03.00.

(30) **Priorité :**

(43) **Date de mise à la disposition du public de la demande :** 14.09.01 Bulletin 01/37.

(56) **Liste des documents cités dans le rapport de recherche préliminaire :** *Se reporter à la fin du présent fascicule*

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

(71) **Demandeur(s) :** *FRANCE TELECOM Société anonyme* — FR et *TELEDIFFUSION DE FRANCE* — FR.

(72) **Inventeur(s) :** MORLET JEAN NOEL.

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

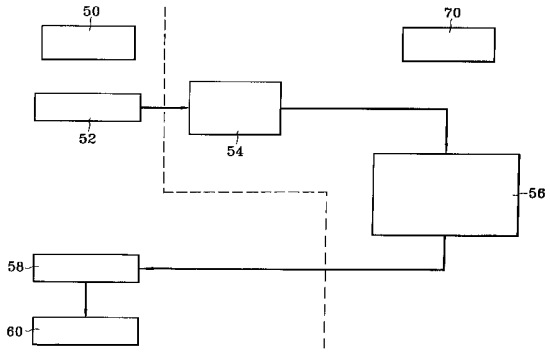
(74) **Mandataire(s) :** BREVALEX.

(54) PROCEDE DE TRANSMISSION D'INFORMATIONS AVEC CONTROLE D'ACCES EN FILIGRANE NUMERIQUE ET DISPOSITIFS DE MISE EN OEUVRE.

(57) Procédé de transmission d'informations avec contrôle d'accès en filigrane numérique.

Les informations de contrôle d'accès sont insérées dans les données embrouillées sous forme de filigrane numérique. A la réception, on extrait des données reçues le filigrane numérique, on retrouve les informations de contrôle d'accès et on désembrouille les données reçues si l'accès est autorisé.

Application, notamment, à la transmission d'images.



FR 2 806 231 - A1

PROCEDE DE TRANSMISSION D'INFORMATIONS AVEC CONTROLE D'ACCES EN FILIGRANE NUMERIQUE ET DISPOSITIFS DE MISE EN OEUVRE

DESCRIPTION

Domaine technique

La présente invention a pour objet un procédé de transmission d'informations avec contrôle d'accès en filigrane numérique et des dispositifs de mise en oeuvre. Elle trouve une application dans la transmission d'images fixes ou animées, d'images d'objets naturels ou de synthèse, de sons, de musique, etc...

Etat de la technique antérieure

La technique de contrôle d'accès est aujourd'hui largement utilisée, notamment dans le domaine de la télévision. Selon cette technique, les informations à transmettre (luminance, chrominance des points d'une image) sont d'abord transformées en données numériques, ces données sont embrouillées par divers algorithmes puis sont émises sous forme embrouillée. Le destinataire est muni d'un processeur de sécurité dans lequel figurent différentes autorisations d'accès à un ou plusieurs services, ainsi que les clés permettant de désembrouiller les données reçues pour restituer l'image d'origine.

Dans cette technique, les informations de contrôle d'accès relatives à un service particulier (référence du service, critères d'accès, clé de désembrouillage chiffrée, ...) sont toujours transmises séparément des

données, ce qui nécessite un protocole spécifique dépendant du type de support de transmission. Par exemple, la façon de transmettre les informations de contrôle d'accès en DVB ("Digital Video Broadcasting") n'a rien de commun avec celle utilisée en DAB ("Digital Audio Broadcasting"). Il y a donc incompatibilité entre ces deux protocoles.

Un but de la présente invention est de remédier à cet inconvénient en supprimant tout protocole de transmission des informations de contrôle d'accès.

Un autre but est d'éviter la piraterie ou la recopie illicite des informations transmises.

Exposé de l'invention

L'invention préconise d'insérer les informations de contrôle d'accès dans les données numériques à transmettre et cela sous une forme particulière, qui est celle du filigrane numérique, appelé également "Watermarking" en anglais. Le filigrane numérique est connu pour marquer une oeuvre afin de la protéger par le droit d'auteur ("Copyright").

De façon précise, l'invention a donc pour objet un procédé de transmission d'informations avec contrôle d'accès, dans lequel, de manière connue :

- à l'émission, on transforme ces informations en données numériques, on embrouille ces données, on transmet les données embrouillées et on transmet en outre des informations de contrôle d'accès,

- à la réception, on reçoit les données embrouillées et les informations de contrôle d'accès et, si l'accès est autorisé, on désembrouille les données reçues et on restitue les informations,

le procédé de l'invention étant caractérisé en ce que :

- à l'émission, les informations de contrôle d'accès sont insérées dans les données numériques sous forme de filigrane numérique et sont émises avec ces données,
- à la réception, on extrait, des données reçues, le filigrane numérique, on retrouve les informations de contrôle d'accès et on désembrouille les données reçues si l'accès est autorisé.

Lorsque les données numériques sont organisées en multiplets (par exemple en octets), les informations de contrôle d'accès du filigrane numérique sont insérées dans certains multiplets, à la place de certain(s) élément(s) binaire(s), par exemple l'élément binaire de plus faible poids. Le choix de ces multiplets est déterminé par une clé.

La transmission des données et du filigrane peut se faire par n'importe quel moyen : par voie hertzienne, par fil, par câble numérique, par support d'enregistrement (par exemple par disque optique numérique dit CD), etc...

Bien que l'invention s'applique à toute forme d'informations, dans un mode privilégié de mise en oeuvre, ces informations correspondent à des images. Dans ce cas, l'embrouillage réalisé est tel que la

qualité d'origine de l'image se trouve dégradée, le désembrouillage redonnant sa qualité d'origine à l'image. Cette dégradation peut s'effectuer par degré selon un indice d'embrouillage.

Dans l'application aux images, la transmission peut s'effectuer à travers le réseau Internet, entre un serveur d'images et un usager pourvu d'un équipement approprié. Dans ce cas :

- l'usager commande une image au serveur d'images,
- le serveur d'images insère un filigrane numérique dans les données numériques de l'image, dégrade la qualité de l'image en embrouillant les données numériques de l'image selon un indice d'embrouillage choisi et transmet l'image de qualité dégradée avec le filigrane numérique,
- l'usager enregistre les données reçues et utilise son équipement pour restituer à l'image sa qualité d'origine et pour afficher l'image commandée.

Il faut souligner enfin une différence fondamentale entre le filigrane numérique classique marquant une image dans le but de préserver le droit d'auteur ("watermarking") et le filigrane utilisé selon la présente invention pour transmettre des conditions d'accès. Dans le premier cas, l'usager peut être tenté de manipuler l'image pour faire disparaître le marquage. Ce marquage peut aussi être perturbé naturellement, voir disparaître, si l'image subit des

dégradations dans la transmission, ou des traitements numériques comme la compression d'image par exemple. Dans l'invention, de telles manipulations ou traitements sont exclus, car l'information liée au filigrane est nécessaire à l'obtention de l'image. En d'autres termes, le filigrane de l'invention n'est plus considéré comme une entrave à l'exploitation de l'information mais comme une nécessité pour la réception de celle-ci.

La présente invention a également pour objet un dispositif pour l'émission d'informations avec contrôle d'accès pour la mise en oeuvre du procédé qui vient d'être décrit. Ce dispositif comprend des moyens pour transformer ces informations en données numériques, des moyens pour embrouiller ces données, des moyens de transmission de ces données embrouillées et d'informations de contrôle d'accès. Ce dispositif est caractérisé en ce qu'il comprend des moyens pour insérer les informations de contrôle d'accès dans les données numériques sous forme de filigrane numérique, les moyens de transmission étant aptes à transmettre les données embrouillées avec les informations de contrôle d'accès.

De préférence, ce dispositif comprend des moyens pour insérer un filigrane numérique dans les données relatives à une image, des moyens pour dégrader la qualité de l'image en embrouillant les données numériques de l'image selon un indice d'embrouillage choisi, et des moyens pour transmettre l'image de qualité dégradée avec le filigrane numérique.

La présente invention a également pour objet un dispositif pour la réception d'informations avec contrôle d'accès pour la mise en oeuvre du procédé déjà défini. Ce dispositif comprend des moyens de réception des données embrouillées et des informations de contrôle d'accès, des moyens pour vérifier si l'accès est autorisé, et des moyens pour désembrouiller les données reçues si l'accès est autorisé et des moyens pour restituer les informations. Le dispositif de l'invention est caractérisé en ce que les moyens de réception sont aptes à extraire des données reçues le filigrane numérique qu'elles contiennent pour retrouver les informations de contrôle d'accès et désembrouiller les données si l'accès est autorisé.

De préférence, les moyens pour désembrouiller les données sont des moyens aptes à restituer à une image de qualité dégradée sa qualité d'origine.

Brève description des dessins

- la figure 1 est un organigramme général illustrant le procédé de l'invention,
- la figure 2 illustre un service de distribution sécurisée d'images sur le réseau Internet.

Description détaillée d'un mode particulier de mise en oeuvre

La description qui suit se rapporte, à titre explicatif, au cas de la transmission d'images de type BMP ("Bit Map Pictures"), mais l'invention n'est nullement limitée à ce cas.

Dans ce mode particulier de mise en oeuvre, le procédé peut mettre en oeuvre deux unités distinctes :

- un serveur d'images comprenant un moyen d'embrouillage de l'image et d'insertion du filigrane numérique contenant les informations de contrôle d'accès et diverses limitations,
- un équipement d'usager possédant une visionneuse ("viewer"), un algorithme d'extraction de filigrane et un algorithme de désembrouillage.

Ces deux unités vont être écrites dans le cas d'un ordinateur personnel (PC) fonctionnant sous les logiciels Windows 95/98 ou NT (marques déposées).

a) Saisie des paramètres de contrôle d'accès pour le serveur

Différents paramètres de contrôle d'accès peuvent être insérés dans l'image sous forme de filigrane numérique, notamment :

- Paramètre désactivation de la copie d'écran : une image désembrouillée par l'équipement de l'usager peut être facilement récupérée par une recopie ou une capture d'écran ; ces fonctions de recopie et de capture d'écran peuvent être désactivées dans l'équipement pour toutes les applications tournant sur l'ordinateur ;
- Paramètre sur la limitation des utilisations : on peut restreindre le nombre d'utilisations d'une image en donnant le nombre maximal

d'utilisations autorisé (WM-NBMAX-UTIL) ainsi que la référence de l'image (WM-REF-IMAGE) ;

- Paramètre sur le destinataire : on peut réserver l'usage à un utilisateur unique en insérant sa référence d'usager (WM-REF-USAGER) ou la référence à un service (WM-REF-SERVICE).

b) Insertion du filigrane numérique

L'image d'origine est une image "bitmap" BMP en codage spatial dans laquelle chaque pixel est représenté par ses trois composantes RVB (Rouge-Vert-Bleu). Le fichier BMP a la structure suivante :

- Un en-tête, dans lequel sont définies les caractéristiques de l'image (taille, pointeur sur le bitmap, nombre de bits de codage, nombre de plans, palette des couleurs, etc...) ;
- Une zone contenant les informations de toute l'image.

Certains octets sont choisis pour recevoir les bits d'information du filigrane, comme il sera expliqué plus loin. Chaque octet ainsi choisi sera appelé par la suite "octet-filigrane". Pour marquer un tel octet, il suffit de remplacer un élément binaire (ou "bit"), par exemple le bit de poids faible (b_0), par l'élément binaire à insérer. La variation de la valeur de l'octet-filigrane par rapport à son ancienne valeur est au maximum de 1/256 ce qui, dans une composante de chrominance, ne se remarque pas à l'œil.

Pour insérer un filigrane composé de n bits dans une zone du bitmap, on divise cette zone en n parties

égales et on marque l'octet correspondant au début de chaque partie ainsi définie. L'adresse de l'octet-filigrane correspondant au bit i à marquer est, par conséquent, l'adresse du début de zone plus la fraction L(i-1)/n où L est la longueur de la zone.

c) Informations insérées dans l'image par filigrane numérique

Les premières informations à insérer sont l'identificateur de filigrane (WM-ID sur six octets) et la longueur des données qui suivent (en octets). Cette longueur (codée sur 8 bits), qui doit être retrouvée systématiquement, est marquée dans la zone d'adresse de début : adresse du début du bitmap et de largeur 300h (la lettre h signifie que les adresses sont exprimées dans un système hexadécimal).

Le reste des données est inséré dans la zone comprise entre l'adresse 300h et l'adresse de fin du bitmap. Cette zone est composée de :

- **WM-DESCR (1 octet)** : descripteur des conditions d'accès, avec les bits suivants :
  - b_0 : copie d'écran interdite
  - b_1 : limitation du nombre d'utilisations
  - b_2 : restriction à certains usagers
  - b_3 : réservé à un usager unique
  - b_4 : réservé à un service

- **WM-MASK (1 octet)** : masque de chiffrement (indice marquant le degré de dégradation de l'image). Il

indique à l'équipement quels sont les bits embrouillés dans le bitmap :

- 00h : image non dégradée
- 1Eh : dégradation faible
- 3Eh : dégradation moyenne
- 7Eh : dégradation forte
- FEh : embrouillage total

La suite des données dépend des sélections effectuées dans la saisie des paramètres de contrôle d'accès. Parmi les cas pouvant se présenter, on peut citer les cas où l'on spécifie :

- un nombre limité d'utilisations
- une exclusivité accordée à un usager unique
- une exclusivité accordée à un service
- un nombre limité d'utilisations ET exclusivité à un usager unique
- un nombre limité d'utilisations ET exclusivité à un service

Ces cas peuvent correspondre aux informations suivantes :

- Nombre limité d'utilisations :

  WM-NBMAX-UTIL (2 octets) : nombre maximal d'utilisations (nombre de bits : 16)

  WM-REF-IMAGE (2 octets) : référence de l'image (nombre de bits : 16)

- Exclusivité à un usager unique

WM-REF-USAGER (2 octets) : référence de l'usager (nombre de bits : 16)

- Exclusivité à un service

WM-REF-SERVICE (8 octets) : référence du service

- Nombre limité d'utilisations ET exclusivité à un usager unique

WM-NBMAX-UTIL (2 octets) : nombre maximal d'utilisations (nombrede bits : 16)

WM-REF-IMAGE (2 octets) : référence de l'image (nombre de bits : 16)

WM-REF-USAGER (2 octets) : référence de l'usager (nombre de bits : 16)

- Nombre limité d'utilisations ET exclusivité à un service

WM-NBMAX-UTIL (2 octets) : nombre maximal d'utilisations (nombre de bits : 16)

WM-REF-IMAGE (2 octets) : référence de l'image (nombre de bits : 16)

WM-REF-SERVICE (8 octets) : référence du service

d) Embrouillage

Dans l'application décrite, l'embrouillage s'obtient grâce à une suite chiffrante initialisée par une clé. Six cas peuvent être envisagés :

- aucun critère de contrôle d'accès : la clé est prise égale à 0,

- nombre limité d'utilisations : la clé est prise égale à la référence de l'image,
- exclusivité à un usager : la clé est prise égale à la référence de l'usager,
- exclusivité à un service : la clé est une fonction de la référence du service,
- nombre limité d'utilisations ET exclusivité à un usager : la clé est la référence de l'usager

L'algorithme d'embrouillage opère sur tous les octets en effectuant une opération logique OU EXCLUSIF (XOR) entre certains bits de l'octet courant et les bits correspondants de l'octet chiffrant de la suite chiffrante. Cet algorithme n'opère que sur les 7 bits non utilisés pour le filigrane, par exemple les 7 bits de poids fort et ne chiffre jamais le bit b_0 de plus faible poids, si c'est celui qui peut contenir un bit du filigrane numérique.

e) Equipement de l'usager

L'équipement de l'usager extrait l'éventuel identificateur WM-ID-LU du filigrane et le vérifie. Si cet identificateur WM-ID-LU ne correspond pas au WM-ID de l'algorithme, l'image ne possède pas d'informations de contrôle d'accès et est considérée comme étant en accès libre.

Si identificateur WM-ID est trouvé, alors l'équipement extrait le filigrane complet et opère chronologiquement de la façon suivante :

- Vérification de la correspondance du destinataire avec les caractéristiques de l'équipement ; vérification éventuelle du sceau cryptographique (appelé aussi "Hash") si le nombre d'utilisations est limité ; s'il n'y a pas de concordance ou si le sceau est faux, l'image n'est pas désembrouillée ;
- Vérification du nombre d'utilisations de l'image (ainsi que son sceau) si le nombre d'utilisations est limité ; si le nombre maximum d'utilisations est dépassé ou si le sceau est faux, l'image n'est pas désembrouillée ;
- Désembrouillage de l'image en utilisant la clé et le masque décrits au paragraphe précédent.

Dans le cas d'une image dont on a fixé un nombre maximal d'utilisations, lors de la première utilisation les informations suivantes sont inscrites dans la base de registre de Windows :

- Référence de l'usager ou référence du service ET du sceau si un destinataire est précisé ;
- Référence de l'image ET du sceau ;
- Nombre d'utilisations restantes ET sceau.

A chaque nouvelle utilisation de l'image, le nombre d'utilisations est décrémenté, le sceau recalculé et le tout est inscrit dans la base de registre de Windows. L'algorithme de sceau utilisé peut être MD5.

Si l'image contient une interdiction de copie d'écran, un ordre d'empêchement ("Hook") est utilisé pour désactiver l'appel à cette fonction.

Ces différentes opérations sont illustrées schématiquement sur les figures 1 et 2.

Sur la figure 1, tout d'abord, le bloc 10 désigne un serveur de droits, qui effectue le chargement et la gestion des droits des différents usagers, symbolisés par la carte 12. Ce chargement peut s'effectuer de quelque manière que ce soit : par fil, voie hertzienne, etc... Côté fournisseur d'images, une carte 20 est une carte mère externe ou un moyen de gestion des droits résidant dans l'applicatif du filigrane numérique. Cette carte commande un bloc 22 relatif au contrôle d'accès. Les données numériques organisées dans le bloc 30 sont dégradées dans le bloc 32. On y insère ensuite les données de contrôle d'accès (bloc 34) et l'ensemble est diffusé comme l'indique symboliquement la flèche 35.

Chez l'usager, on détecte la présence de données dans le filigrane (36) et si cette présence est détectée, on extrait les données en question (38). Sinon, on décide (44) d'utiliser les données brutes. Les données extraites sont vérifiées dans le bloc 46, qui reçoit par ailleurs les droits inscrits dans la carte 12. Ces droits font ensuite l'objet d'une vérification des conditions d'accès (48). Si les conditions d'accès sont vérifiées, les données sont désembrouillées (40) et ces données désembrouillées sont utilisées pour afficher l'image (42). Si les

conditions d'accès ne sont pas vérifiées, on revient à l'utilisation des données brutes.

La figure 2, quant à elle, illustre plus spécialement le principe d'un service de distribution sécurisée d'images sur le réseau Internet. Côté usager, symbolisé par le bloc 50, la première opération est une commande (52) d'une image. Côté serveur d'images, symbolisé par le bloc 70, on constitue (54) une référence d'image, une référence d'usager, et des conditions d'accès. Puis on fabrique une image dégradée et on y insère par filigrane numérique la référence d'image, la référence d'usager et les conditions d'accès (bloc 56). L'ensemble de toutes ces données est adressé à l'usager où elles sont enregistrées dans le fichier (58). Les données sont ensuite traitées et exploitées (60) dans l'équipement de l'usager.

REVENDICATIONS

1. Procédé de transmission d'informations avec contrôle d'accès, dans lequel :

- à l'émission, on transforme ces informations en données numériques, on embrouille ces données, on transmet les données embrouillées et on transmet en outre des informations de contrôle d'accès,
- à la réception, on reçoit les données embrouillées et les informations de contrôle d'accès et, si l'accès est autorisé, on désembrouille les données reçues et on restitue les informations,

caractérisé en ce que :

- à l'émission, les informations de contrôle d'accès sont insérées dans les données numériques sous forme de filigrane numérique et sont émises avec ces données,
- à la réception, on extrait, des données reçues, le filigrane numérique, on retrouve les informations de contrôle d'accès et on désembrouille les données reçues si l'accès est autorisé.

2. Procédé selon la revendication 1, dans lequel, les informations numériques étant organisées en multiplets, les informations de contrôle d'accès du filigrane numérique sont insérées dans certains multiplets, à la place de certain(s) élément(s) binaire(s) de ces multiplets.

3. Procédé selon la revendication 2, dans lequel l'élément binaire utilisé pour le filigrane est l'élément binaire de plus faible poids.

4. Procédé selon la revendication 2, dans lequel l'embrouillage affecte les éléments binaires de chaque multiplet autres que le(s) élément(s) binaire(s) servant au filigrane.

5. Procédé selon l'une quelconque des revendications 2 à 4, dans lequel les multiplets sont des octets.

6. Procédé selon la revendication 1, dans lequel les informations de contrôle d'accès insérées sous forme de filigrane numérique contiennent les informations suivantes :

- un identificateur de filigrane numérique,
- la longueur du filigrane numérique,
- des descripteurs de conditions d'accès.

7. Procédé selon la revendication 6, dans lequel les informations de contrôle d'accès insérées sous forme de filigrane numérique contiennent, en outre, au moins l'une des informations suivantes :

- un nombre limité d'utilisations des données,
- une réserve pour un usager particulier seul autorisé à recevoir les données,
- une réserve à un service particulier seul autorisé à recevoir les données.

8. Procédé selon l'une quelconque des revendications 1 à 7, dans lequel les informations sont relatives à des images.

9. Procédé selon la revendication 8, dans lequel les informations de contrôle d'accès contiennent une instruction interdisant la recopie de l'image.

10. Procédé selon la revendication 8, dans lequel les informations de contrôle d'accès contiennent une instruction désactivant une copie d'écran.

11. Procédé selon la revendication 8, dans lequel l'embrouillage dégrade la qualité de l'image et dans lequel le désembrouillage redonne sa qualité à l'image.

12. Procédé selon la revendication 11, dans lequel la dégradation de la qualité de l'image s'effectue par degré selon un indice d'embrouillage.

13. Procédé selon la revendication 1, dans lequel la transmission s'effectue par des moyens hertziens, ou par fil, ou par câble numérique, ou par support d'enregistrement numérique.

14. Procédé selon la revendication 13, dans lequel la transmission s'effectue par le réseau Internet entre un serveur d'images et un usager pourvu d'un équipement approprié.

15. Procédé selon la revendication 14, dans lequel :

- l'usager commande une image au serveur d'images,
- le serveur d'images insère un filigrane numérique dans les données de l'image, dégrade la qualité de l'image en embrouillant les données numériques de l'image commandée selon un indice d'embrouillage choisi, et transmet l'image de qualité dégradée avec le filigrane numérique,
- l'usager enregistre les données reçues et utilise son équipement pour restituer à l'image sa qualité d'origine et afficher l'image commandée.

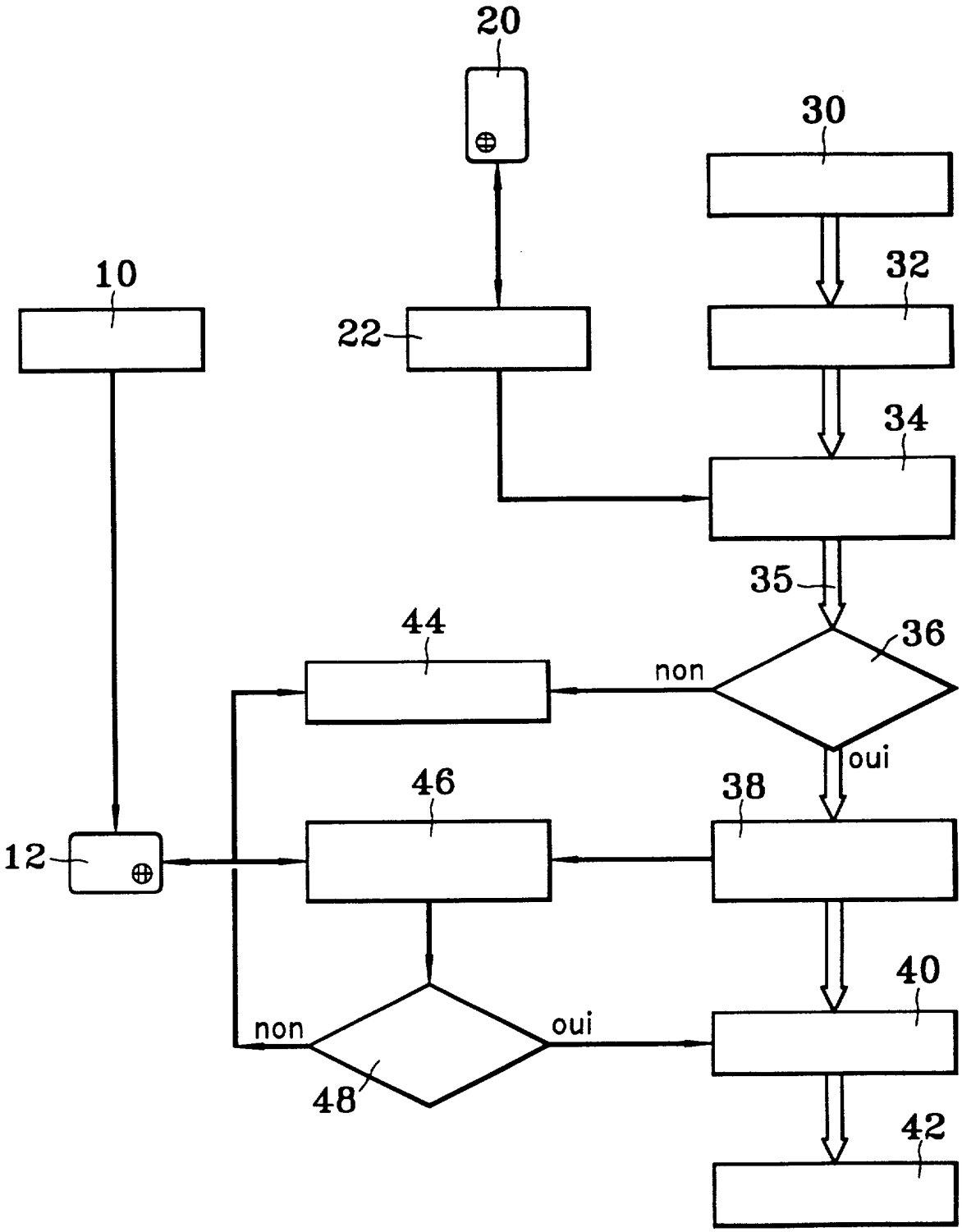
16. Dispositif pour l'émission d'informations avec contrôle d'accès pour la mise en oeuvre du procédé selon la revendication 1, ce dispositif comprenant des moyens pour transformer ces informations en données numériques, des moyens pour embrouiller ces données, des moyens de transmission de ces données embrouillées et d'informations de contrôle d'accès, caractérisé en ce qu'il comprend des moyens pour insérer les informations de contrôle d'accès dans les données numériques sous forme de filigrane numérique, les moyens de transmission étant aptes à transmettre les données embrouillées avec les informations de contrôle d'accès.

17. Dispositif selon la revendication 16, comprenant des moyens pour insérer un filigrane numérique dans les données relatives à une image, des moyens pour dégrader la qualité de l'image en embrouillant les données numériques de l'image selon un indice d'embrouillage choisi, et des moyens pour transmettre l'image de qualité dégradée avec le filigrane numérique.

18. Dispositif pour la réception d'informations avec contrôle d'accès pour la mise en oeuvre du procédé selon la revendication 1, ce dispositif comprenant des moyens de réception des données embrouillées et des informations de contrôle d'accès, des moyens pour vérifier si l'accès est autorisé, et des moyens pour désembrouiller les données reçues si l'accès est autorisé et des moyens pour restituer les informations, caractérisé en ce que les moyens de réception sont aptes à extraire des données reçues le filigrane numérique qu'elles contiennent pour retrouver les informations de contrôle d'accès et désembrouiller les données si l'accès est autorisé.

19. Dispositif selon la revendication 18, dans lequel les moyens pour désembrouiller les données sont des moyens aptes à restituer à une image de qualité dégradée sa qualité d'origine.

FIG. 1



2806231

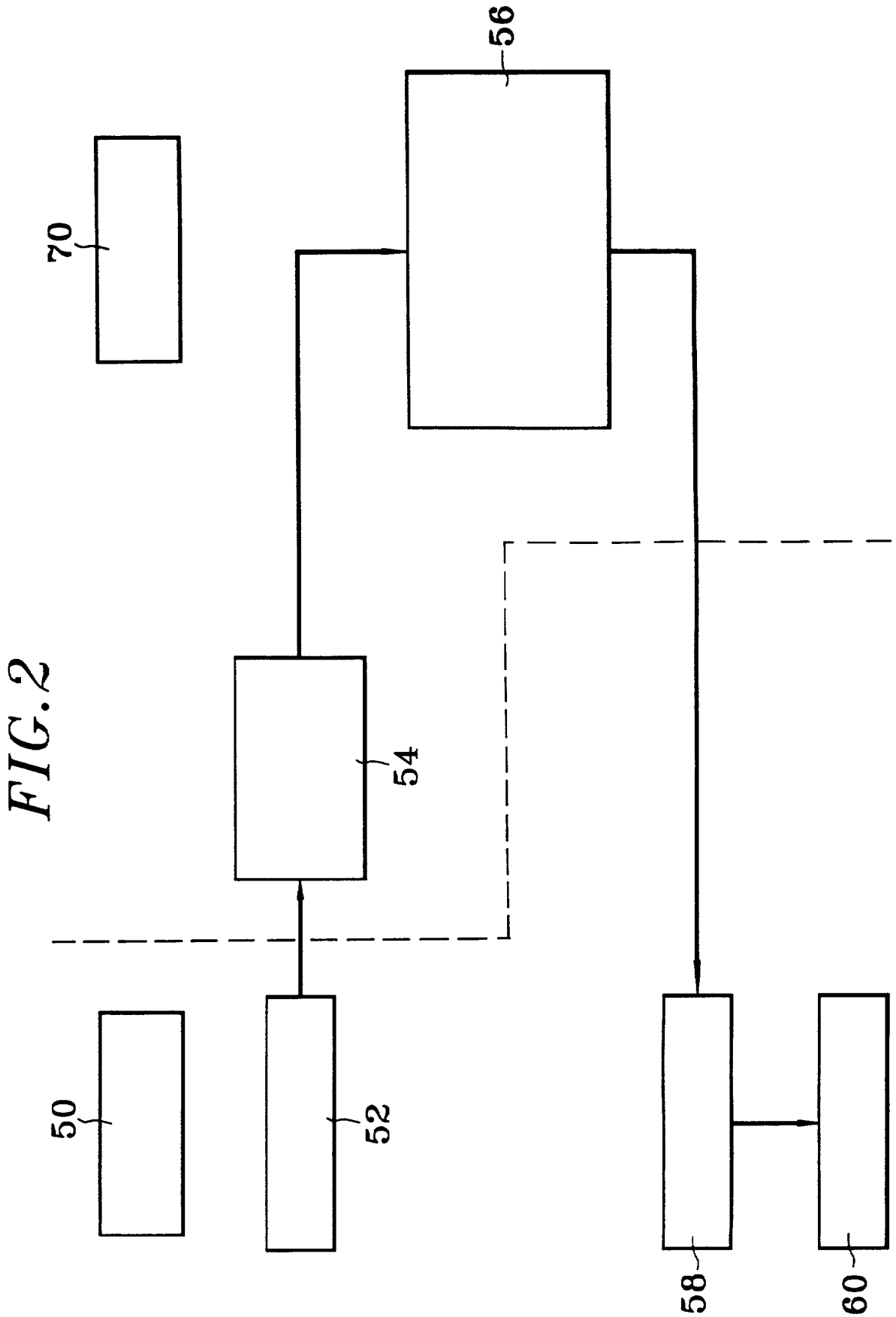


FIG. 2

RÉPUBLIQUE FRANÇAISE

INPI
INSTITUT NATIONAL DE LA PROPRIETE INDUSTRIELLE

2806231

N° d'enregistrement national

FA 583690
FR 0002960

RAPPORT DE RECHERCHE PRÉLIMINAIRE

établi sur la base des dernières revendications déposées avant le commencement de la recherche

DOCUMENTS CONSIDÉRÉS COMME PERTINENTS		Revendication(s) concernée(s)	Classement attribué à l'invention par l'INPI
Catégorie	Citation du document avec indication, en cas de besoin, des parties pertinentes		
E	WO 00 52923 A (KALKER ANTONIUS A C M ;KONINKL PHILIPS ELECTRONICS NV (NL)) 8 septembre 2000 (2000-09-08) * le document en entier * ---	1,16	H04L9/32 H04N1/32
Y	US 4 742 544 A (MOOTE STANLEY R ET AL) 3 mai 1988 (1988-05-03) * abrégé * ---	1,8,9, 11,13, 16,18,19	
Y	WO 99 10858 A (LEIGHTON F THOMSON) 4 mars 1999 (1999-03-04)	1,8,9, 11,13, 16,18,19	
A	* le document en entier * ---	7	
A	WO 99 57885 A (KOCH ECKHARD ;MEDIASEC TECHNOLOGIES LLC (US); FRAUNHOFER CENTER FO) 11 novembre 1999 (1999-11-11) * le document en entier * ---	1	
A	SCHYNDEL VAN R G ET AL: "A DIGITAL WATERMARK" AUSTIN, NOV. 13 - 16, 1994,LOS ALAMITOS, IEEE COMP. SOC. PRESS,US, vol. CONF. 1, 13 novembre 1994 (1994-11-13), pages 86-90, XP000522615 ISBN: 0-8186-6952-7 * abrégé * -----	2,3	DOMAINES TECHNIQUES RECHERCHÉS (Int.CL.7) H04N

Date d'achèvement de la recherche	Examinateur
21 novembre 2000	Hazel, J

CATÉGORIE DES DOCUMENTS CITÉS

X : particulièrement pertinent à lui seul
Y : particulièrement pertinent en combinaison avec un autre document de la même catégorie
A : arrière-plan technologique
O : divulgation non-écrite
P : document intercalaire

T : théorie ou principe à la base de l'invention
E : document de brevet bénéficiant d'une date antérieure à la date de dépôt et qui n'a été publié qu'à cette date de dépôt ou qu'à une date postérieure.
D : cité dans la demande
L : cité pour d'autres raisons

& : membre de la même famille, document correspondant

EPO FORM 1503 12.99 (P04C14)