(12) DEMANDE INTERNATIONALE PUBLIÉE EN VERTU DU TRAITÉ DE COOPÉRATION EN MATIÈRE DE BREVETS (PCT)

(19) Organisation Mondiale de la Propriété Intellectuelle
Bureau international

PCT

(43) Date de la publication internationale
26 mars 2009 (26.03.2009)

(10) Numéro de publication internationale
WO 2009/037133 A1

(51) Classification internationale des brevets :
H04L 9/32 (2006.01) *H04N 1/32* (2006.01)
G01S 1/00 (2006.01)

(21) Numéro de la demande internationale :
PCT/EP2008/061780

(22) Date de dépôt international :
5 septembre 2008 (05.09.2008)

(25) Langue de dépôt : français

(26) Langue de publication : français

(30) Données relatives à la priorité :
07 06643 21 septembre 2007 (21.09.2007) FR

(71) Déposant *(pour tous les États désignés sauf US)* : **THALES** [FR/FR]; 45, rue de Villiers, F-92200 Neuilly Sur Seine (FR).

(72) Inventeur; et

(75) Inventeur/Déposant *(pour US seulement)* : **DAMIDAUX, Jean-Louis** [FR/FR]; 5, hameau du Crouzet, F-31650 Auzielle (FR).

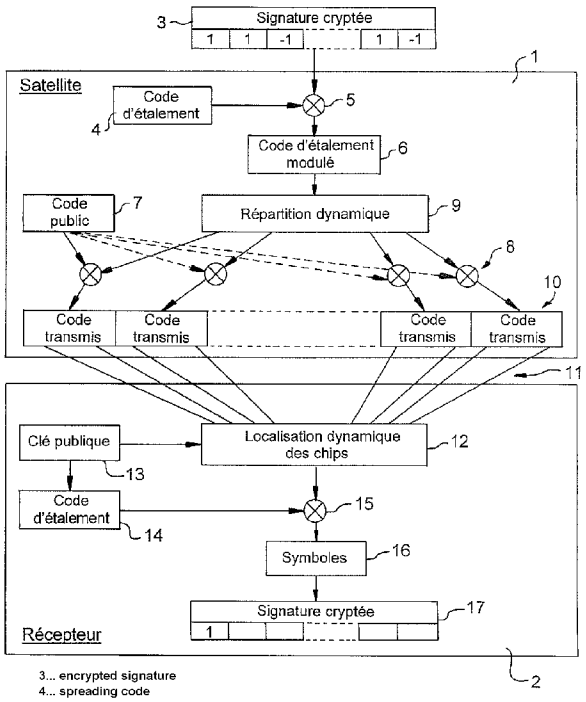
(74) Mandataires : **BREDA, Jean-Marc** etc.; Marks & Clerk France, Conseils en Propriété Industrielle, Immeuble "Visium", 22, avenue Aristide Briand, F-94117 Arcueil Cedex (FR).

(81) États désignés *(sauf indication contraire, pour tout titre de protection nationale disponible)* : AE, AG, AL, AM, AO,

[Suite sur la page suivante]

(54) Title: METHOD PROVIDING THE MEANS FOR RECOGNIZING THE ORIGIN AND/OR CONTENT OF AN RF SIGNAL

(54) Titre : PROCEDE FOURNISSANT LES MOYENS DE RECONNAITRE L'ORIGINE ET/OU LE CONTENU D'UN SIGNAL RF



3... encrypted signature
4... spreading code
6... modulated spreading code
7... public code
9... dynamic distribution
10... code transmitted
13... public key
14... spreading code
2... receiver
12... dynamic location of chips
16... symbols
17... encrypted signature

(57) Abstract: The subject of the present invention is a method providing the means making it possible to recognize the origin and/or content of an RF signal without requiring substantial means of calculation, these recognition means being accessible only to authorized persons and being practically non-modifiable and very difficult to detect by unauthorized persons, this being the case in various applications implementing RF signals transmitting information that is at least in part hidden. This method is characterized in that it spreads an item of information to be hidden with the aid of a hidden code, and the information thus obtained is distributed with the aid of an Exclusive OR function in codes which are known with the aid of a hidden distribution algorithm, in that on reception the inverse algorithm to that which served for distribution is implemented so as to access the spread code, and in that this spread code is correlated with the hidden code so as to retrieve the hidden item of information.

(57) Abrégé : La présente invention a pour objet un procédé fournissant les moyens permettant de reconnaître l'origine et/ou le contenu d'un signal RF sans nécessiter d'importants moyens de calcul, ces moyens de reconnaissance n'étant accessibles qu'à des personnes autorisées et étant pratiquement non modifiables et très difficilement détectables par des personnes non autorisées, et ce, dans diverses applications mettant en œuvre des signaux RF transmettant des informations au moins en partie cachées. Ce procédé est caractérisé en ce qu'on étale une information à cacher à l'aide d'un code caché, qu'on répartit, à l'aide d'une fonction OU Exclusif l'information ainsi obtenue dans des codes connus à l'aide d'un algorithme de répartition caché,

[Suite sur la page suivante]

WO 2009/037133 A1

AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) États désignés *(sauf indication contraire, pour tout titre de protection régionale disponible)* **:** ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), eurasien (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), européen (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MT, NL, NO, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Publiée :

— *avec rapport de recherche internationale*

qu'à la réception on met en œuvre l'algorithme inverse de celui ayant servi à la répartition pour accéder au code étalé, qu'on corrèle ce code étalé avec le code caché pour retrouver l'information cachée.

PROCEDE FOURNISSANT LES MOYENS DE RECONNAITRE L'ORIGINE ET/OU LE CONTENU D'UN SIGNAL RF

La présente invention se rapporte à un procédé fournissant les moyens permettant de reconnaître l'origine et/ou le contenu d'un signal RF.

On connaît de nombreuses techniques pour combattre le brouillage de signaux tels que ceux des radars. Par contre, dans un domaine tel que celui de la réception de signaux de radio-localisation, il faut disposer des mesures (dites pseudo-mesures) fournies par des satellites et de données d'éphéméride. Il est relativement facile de protéger les données d'éphéméride pour en garantir l'origine et/ou le contenu. Par contre, les caractéristiques des signaux de mesure sont dans le domaine public, et ne peuvent donc être protégés. Il est alors facile d'émuler ces signaux afin qu'un utilisateur obtienne des coordonnées de position géographique fausses. Il en est de même dans d'autres domaines de transmissions numériques tels que les télécommunications ou les diffusions de programmes de télévision.

Peu de recherches ont été menées pour permettre de garantir l'origine de tels signaux RF. En effet, il est maintenant possible, si l'on met en œuvre des calculateurs suffisamment puissants, de produire de façon malintentionnée des signaux imitant ceux émis par les satellites de géo-localisation. Ces techniques de leurrage sont dénommées en anglais « spoofing ».

Quelques indications pour essayer d'authentifier les signaux reçus ont été décrites par exemple dans un article de Logan SCOTT « Anti-Spoofing and Authenticated Signal Architectures for Civil Navigation systems » paru dans la revue ION GPS/GNSS 2003, 9-12 Septembre 2003, Portland, OR. Toutefois, la détermination de l'origine et/ou du contenu des signaux reçus nécessite également d'importants moyens de calcul consommant une énergie non négligeable et n'est donc pas à la portée d'un simple utilisateur d'un récepteur de radio-navigation ou d'un utilisateur ordinaire abonné à des programmes de télévision numérique.

La présente invention a pour objet un procédé fournissant les moyens permettant de reconnaître l'origine et/ou le contenu d'un signal RF sans nécessiter d'importants moyens de calcul, ces moyens de reconnaissance n'étant accessibles qu'à des personnes autorisées et étant pratiquement non modifiables et très

difficilement détectables par des personnes non autorisées, et ce, dans diverses applications mettant en œuvre des signaux RF transmettant des informations au moins en partie cachées.

Le procédé conforme à l'invention est caractérisé en ce qu'on étale une information à cacher à l'aide d'un code caché, qu'on répartit cette information, à l'aide d'une fonction XOR (OU Exclusif), dans des codes connus à l'aide d'un algorithme de répartition caché, qu'à la réception on met en œuvre l'algorithme inverse de celui ayant servi à la répartition pour accéder au code étalé, qu'on corrèle ce code étalé avec le code caché pour retrouver l'information cachée. De façon avantageuse, le code caché est décalé au moment de l'émission, afin qu'à la réception, lors de la corrélation de ce code étalé avec le code caché non décalé, le décalage soit détecté. La valeur de ce décalage peut permettre de transmettre de l'information.

La présente invention sera mieux comprise à la lecture de la description détaillée d'un mode de réalisation, pris à titre d'exemple non limitatif et illustré par le dessin annexé, sur lequel :

- la figure unique est un bloc-diagramme simplifié d'un dispositif de mise en œuvre du procédé de l'invention.

L'invention est décrite ci-dessous en référence à la vérification de l'origine et/ou du contenu de signaux de radio-localisation (GNSS), mais il est bien entendu qu'elle n'est pas limitée à cette seule application, et qu'elle peut être mise en œuvre pour différents signaux RF, tels que d'autres types de signaux de localisation (terrestres par exemple) ou des signaux de télévision numérique terrestre (TNT), en particulier de télévision payante, ou encore des signaux de téléphonie payante.

Une caractéristique essentielle du procédé de l'invention est de cacher dans la séquence d'étalement une signature numérique que l'on peut qualifier de filigrane (« watermark » en anglais). Ce filigrane est caché de façon qu'on ne puisse pas le détecter directement ou à l'aide de méthodes statistiques dans la séquence d'étalement. Bien entendu, un utilisateur autorisé peut facilement extraire ce filigrane de la séquence d'étalement et s'en servir pour déterminer la source du signal reçu.

Sur le bloc-diagramme de la figure unique du dessin, montrant un satellite 1 et un des récepteurs correspondants 2, on n'a représenté que les éléments relatifs à l'invention.

Les circuits appropriés du satellite 1 reçoivent une information 3 de signature cachée qui peut être stockée à bord ou transmise depuis le sol. Cette signature est une information cachée connue uniquement de l'organisme contrôlant le satellite et des utilisateurs habilités à la connaître (par exemple les abonnés à un service payant transmis par le satellite 1). La signature 3 comporte une longue séquence, de préférence d'une centaine de bits au moins, qui permet de reconnaître l'origine et/ou le contenu de signaux de radio-localisation et est avantageusement modifiable dynamiquement depuis le sol à l'aide de messages cryptés en envoyant soit une nouvelle séquence, soit une nouvelle graine pour générer une nouvelle séquence, soit un ordre de changement de signature parmi celles stockées à bord. Un code caché d'étalement (filigrane) 4 est « modulé » (5) par cette signature (3). Cette modulation consiste à étaler le filigrane tout au long de la séquence de la signature 3. On obtient ainsi un filigrane modulé 6. Ce code 4 d'étalement est un code privé qui peut lui aussi être modifié dynamiquement depuis le sol comme décrit ci-dessus pour la signature 3.

On modifie ensuite (de façon difficilement détectable, comme précisé ci-dessous) une partie d'un code public 7, qui est ici un code d'étalement de navigation classique, à l'aide d'une technique faisant appel au filigrane modulé 6 et à une fonction « OU Exclusif » 8 (également dénommée « XOR »). Cette modification consiste à inverser dynamiquement certains des éléments (« chips » en anglais) du code 7, c'est-à-dire que cette modification est effectuée au fur et à mesure du déroulement du code 6, le code 7 étant présenté aux différentes cellules de la fonction 8 à chaque séquence du filigrane modulé 6, l'emplacement de ces éléments au sein du code public étant déterminé par un algorithme 9 qui utilise des clés privées. Ces éléments sont choisis par l'algorithme de façon pseudo-aléatoire et constituent une faible partie du code public 7, avantageusement quelques pour-cents de ce code, afin de rendre très difficile la détection des modifications de ce code 7 et de dégrader d'une façon minimale la corrélation du code public 7. Le code modulé 6 ayant une longueur supérieure à celle du code 7 et ne modifiant qu'une faible partie de celui-ci, la fonction XOR 8 emploie plusieurs cellules réalisant chacune en temps réel l'opération XOR sur le code 7 qui est présenté à chacune d'elles.

Le code de navigation ainsi caché est diffusé (11) par l'émetteur (non représenté) du satellite 1. Il est traité selon des opérations inverses de celles qui ont été pratiquées à l'émission dans un récepteur de radio-navigation 2, de la façon suivante. Les circuits de réception (non représentés) du récepteur 2 transmettent les signaux reçus du satellite 1 à une entité 12 qui sélectionne dynamiquement à l'aide de la clé publique 13 l'emplacement des chips où l'opération 8 de « OU exclusif » (XOR) a été réalisée.

D'autre part, la clé 13 permet de générer le code caché 14 d'étalement de filigrane (identique au code 4). Ce code 14 est envoyé à un corrélateur 15 qui reçoit de l'entité 12 des séquences de codes dans lesquelles les chips du code 7 modifiés à l'émission ont été rétablis à leurs valeurs d'origine. A la sortie du corrélateur 15, si le code d'étalement 14 est effectivement présent dans le signal reçu, on obtient les symboles (16) qui doivent permettre de reconstituer la signature 17 après décodage, qui doit être identique à la signature 3 si les informations reçues du satellite 1 sont bien celles émises par l'organisme contrôlant le satellite, et non pas un leurre.

En conclusion, la mise en œuvre du procédé de l'invention est « transparente » pour l'utilisateur qui n'a pas besoin des services (en général payants) protégés par ce procédé. Le marquage effectué par ce procédé est très difficilement détectable du fait que le code transmis (10) ainsi modifié n'est quasiment pas altéré et que le code public d'étalement de navigation (7) n'est pas modifié.

En outre, même si des personnes malintentionnées mettaient en œuvre des moyens très importants pour simuler ce marquage, elles seraient obligées d'utiliser une antenne à très grand gain pour détecter les chips modifiés, car sans elle, il est impossible de moduler les signaux de navigation avec les chips modifiés. Il ne serait possible que de différer l'émission des leurres pour avoir le temps d'extraire chaque chip et de l'analyser, mais alors, la vérification de la cohérence Doppler de ces signaux peut être facilement effectuée. Un utilisateur averti peut vérifier la cohérence des signaux reçus (en Doppler et distance, et les valeurs d'éphéméride). Du fait que la valeur des chips modifiés dépend également des données émises, même s'il est possible à des personnes malintentionnées de détecter des chips modifiés, il leur est impossible d'introduire des leurres car ils ne peuvent pas déterminer à quels emplacements ils doivent modifier les chips car s'ils veulent transmettre la valeur opposée à la valeur transmise par le système réel, ils ne connaissent que l'emplacement des chips à ne pas modifier.

REVENDICATIONS

1. Procédé fournissant les moyens permettant de reconnaître l'origine et/ou le contenu d'un signal RF, caractérisé en ce qu'on étale (5) une information à cacher (3) à l'aide d'un code caché (4), qu'on répartit, à l'aide d'une fonction « OU Exclusif » (8) l'information ainsi obtenue dans des codes connus à l'aide d'un algorithme de répartition caché (9), qu'à la réception on met en œuvre l'algorithme inverse (12) de celui ayant servi à la répartition pour accéder au code étalé (14), qu'on corrèle (15) ce code étalé avec le code caché pour retrouver l'information cachée.
2. Procédé selon la revendication 1, caractérisé en ce que le code caché (4) est décalé dans le temps à l'émission.
3. Procédé selon la revendication 2, caractérisé en ce qu'à la réception, lors de la corrélation du code étalé avec le code caché non décalé, on détecte le décalage.
4. Procédé selon la revendication 2 ou 3, caractérisé en ce que le décalage est utilisé pour transmettre de l'information.
5. Procédé selon l'une des revendications précédentes, caractérisé en ce que le signal RF est un signal de radio-localisation d'une constellation de satellites.
6. Procédé selon la revendication 5, caractérisé en ce que l'information à cacher est stockée à bord des satellites.
7. Procédé selon la revendication 5, caractérisé en ce que l'information à cacher est transmise depuis le sol aux satellites.
8. Procédé selon l'une des revendications précédentes, caractérisé en ce que l'information à cacher (3), qui est une longue séquence de bits, est modifiée dynamiquement depuis le sol à l'aide de messages cryptés.
9. Procédé selon la revendication 8, caractérisé en ce que l'information à cacher est modifiée par l'envoi d'une nouvelle séquence.

10. Procédé selon la revendication 8, caractérisé en ce que l'information à cacher est modifiée par l'envoi d'une nouvelle graine pour générer une nouvelle séquence.

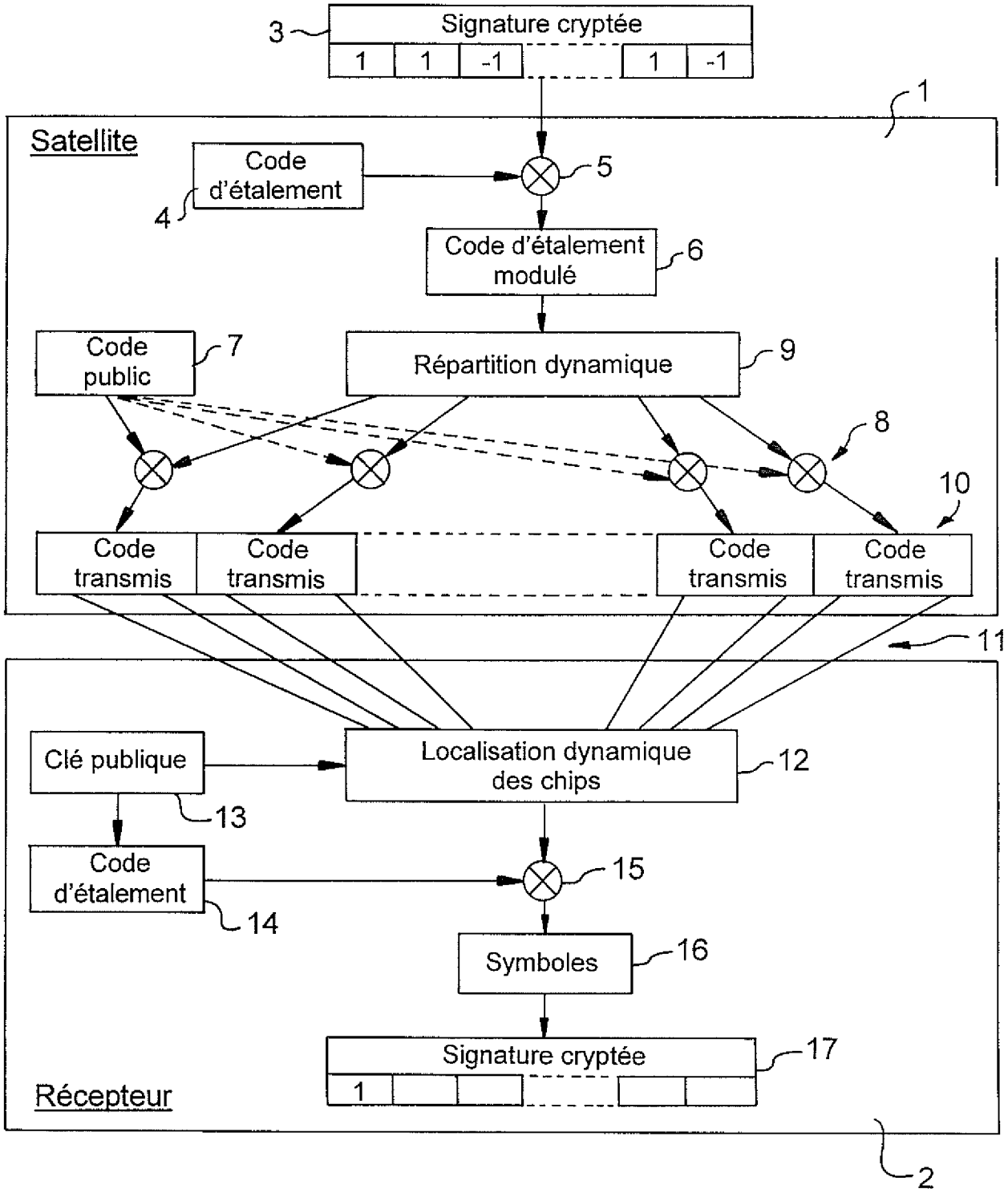
11. Procédé selon la revendication 6, caractérisé en ce que l'on stocke à bord plusieurs informations à cacher et qu'on envoie un ordre de changement pour sélectionner l'une de celles stockées à bord.

12. Procédé selon l'une des revendications 5 à 11, caractérisé en ce que le code caché d'étalement (4) est modifié dynamiquement depuis le sol à l'aide de messages cryptés.

13. Procédé selon la revendication 12, caractérisé en ce que le code caché, qui est une longue séquence de bits, est modifié par l'envoi d'une nouvelle séquence.

14. Procédé selon la revendication 12, caractérisé en ce que le code caché est modifié par l'envoi d'une nouvelle graine pour générer une nouvelle séquence.

15. Procédé selon la revendication 12, caractérisé en ce que l'on stocke à bord plusieurs codes cachés et qu'on envoie un ordre de changement pour sélectionner l'un de ceux stockés à bord.


3
Signature cryptée
1
1
-1
1
-1
1
Satellite
Code d'étalement
4
5
Code d'étalement modulé
6
Code public
7
Répartition dynamique
9
8
10
Code transmis
Code transmis
Code transmis
Code transmis
11
Clé publique
Localisation dynamique des chips
12
13
Code d'étalement
14
15
Symboles
16
Signature cryptée
17
1
Récepteur
2

INTERNATIONAL SEARCH REPORT

International application No
PCT/EP2008/061780

A. CLASSIFICATION OF SUBJECT MATTER
INV. H04L9/32 G01S1/00 H04N1/32

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
H04L G01S H04B H04N H04K

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal, IBM-TDB, INSPEC, COMPENDEX

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	WO 2004/002160 A (KONINKL PHILIPS ELECTRONICS NV [NL]; ROBERTS DAVID K [GB]) 31 December 2003 (2003-12-31)	1
A	abstract page 4, line 15 - page 5, line 25	2-15
X	EP 1 594 122 A (THOMSON BRANDT GMBH [DE]) 9 November 2005 (2005-11-09)	1
A	abstract	2-15
X	INGEMAR J COX ET AL: "Secure Spread Spectrum Watermarking for Multimedia" IEEE TRANSACTIONS ON IMAGE PROCESSING, IEEE SERVICE CENTER, PISCATAWAY, NJ, US, vol. 6, no. 12, 1 December 1997 (1997-12-01), XP011026243 ISSN: 1057-7149	1
A	abstract	2-15

-/--

[X] Further documents are listed in the continuation of Box C. [X] See patent family annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier document but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
4 novembre 2008	11/11/2008

Name and mailing address of the ISA/	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31–70) 340–2040, Fax: (+31–70) 340–3016	Cretaine, Philippe

INTERNATIONAL SEARCH REPORT

International application No
PCT/EP2008/061780

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 7 194 620 B1 (HAYES DAVID SCOTT [US]) 20 March 2007 (2007-03-20) column 5, line 29 - column 6, line 39	1-15
A	US 7 020 555 B1 (JANKY JAMES M [US] ET AL) 28 March 2006 (2006-03-28) abstract	1-15
A	US 2002/191809 A1 (KIROVSKI DARKO [US] ET AL) 19 December 2002 (2002-12-19) abstract	1-15

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/EP2008/061780

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 2004002160 A	31-12-2003	AU 2003239735 A1	06-01-2004
		CN 1663275 A	31-08-2005
		EP 1518411 A1	30-03-2005
		JP 2005531187 T	13-10-2005
		US 2005246536 A1	03-11-2005
EP 1594122 A	09-11-2005	NONE	
US 7194620 B1	20-03-2007	NONE	
US 7020555 B1	28-03-2006	US 7089113 B1	08-08-2006
US 2002191809 A1	19-12-2002	US 2005097333 A1	05-05-2005
		US 2005097334 A1	05-05-2005

RAPPORT DE RECHERCHE INTERNATIONALE

Demande internationale n°
PCT/EP2008/061780

A. CLASSEMENT DE L'OBJET DE LA DEMANDE
INV. H04L9/32 G01S1/00 H04N1/32

Selon la classification internationale des brevets (CIB) ou à la fois selon la classification nationale et la CIB

B. DOMAINES SUR LESQUELS LA RECHERCHE A PORTE

Documentation minimale consultée (système de classification suivi des symboles de classement)
H04L G01S H04B H04N H04K

Documentation consultée autre que la documentation minimale dans la mesure où ces documents relèvent des domaines sur lesquels a porté la recherche

Base de données électronique consultée au cours de la recherche internationale (nom de la base de données, et si cela estréalisable, termes de recherche utilisés)
EPO-Internal, IBM-TDB, INSPEC, COMPENDEX

C. DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie*	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
X	WO 2004/002160 A (KONINKL PHILIPS ELECTRONICS NV [NL]; ROBERTS DAVID K [GB]) 31 décembre 2003 (2003-12-31)	1
A	abrégé page 4, ligne 15 - page 5, ligne 25	2-15
X	EP 1 594 122 A (THOMSON BRANDT GMBH [DE]) 9 novembre 2005 (2005-11-09)	1
A	abrégé	2-15
X	INGEMAR J COX ET AL: "Secure Spread Spectrum Watermarking for Multimedia" IEEE TRANSACTIONS ON IMAGE PROCESSING, IEEE SERVICE CENTER, PISCATAWAY, NJ, US, vol. 6, no. 12, 1 décembre 1997 (1997-12-01), XP011026243 ISSN: 1057-7149	1
A	abrégé	2-15

-/--

[X] Voir la suite du cadre C pour la fin de la liste des documents

[X] Les documents de familles de brevets sont indiqués en annexe

* Catégories spéciales de documents cités:

"A" document définissant l'état général de la technique, non considéré comme particulièrement pertinent

"E" document antérieur, mais publié à la date de dépôt international ou après cette date

"L" document pouvant jeter un doute sur une revendication de priorité ou cité pour déterminer la date de publication d'une autre citation ou pour une raison spéciale (telle qu'indiquée)

"O" document se référant à une divulgation orale, à un usage, à une exposition ou tous autres moyens

"P" document publié avant la date de dépôt international, mais postérieurement à la date de priorité revendiquée

"T" document ultérieur publié après la date de dépôt international ou la date de priorité et n'appartenenant pas à l'état de la technique pertinent, mais cité pour comprendre le principe ou la théorie constituant la base de l'invention

"X" document particulièrement pertinent; l'invention revendiquée ne peut être considérée comme nouvelle ou comme impliquant une activité inventive par rapport au document considéré isolément

"Y" document particulièrement pertinent; l'invention revendiquée ne peut être considérée comme impliquant une activité inventive lorsque le document est associé à un ou plusieurs autres documents de même nature, cette combinaison étant évidente pour une personne du métier

"&" document qui fait partie de la même famille de brevets

Date à laquelle la recherche internationale a été effectivement achevée	Date d'expédition du présent rapport de recherche internationale
4 novembre 2008	11/11/2008

Nom et adresse postale de l'administration chargée de la recherche internationale	Fonctionnaire autorisé
Office Européen des Brevets, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31-70) 340-2040, Fax: (+31-70) 340-3016	Cretaine, Philippe

RAPPORT DE RECHERCHE INTERNATIONALE

Demande internationale n°.
PCT/EP2008/061780

C(suite). DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie*	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
A	US 7 194 620 B1 (HAYES DAVID SCOTT [US]) 20 mars 2007 (2007-03-20) colonne 5, ligne 29 - colonne 6, ligne 39	1-15
A	US 7 020 555 B1 (JANKY JAMES M [US] ET AL) 28 mars 2006 (2006-03-28) abrégé	1-15
A	US 2002/191809 A1 (KIROVSKI DARKO [US] ET AL) 19 décembre 2002 (2002-12-19) abrégé	1-15

RAPPORT DE RECHERCHE INTERNATIONALE

Renseignements relatifs aux membres de familles de brevets

Demande internationale n°
PCT/EP2008/061780

Document brevet cité au rapport de recherche	Date de publication	Membre(s) de la famille de brevet(s)	Date de publication
WO 2004002160 A	31-12-2003	AU 2003239735 A1	06-01-2004
		CN 1663275 A	31-08-2005
		EP 1518411 A1	30-03-2005
		JP 2005531187 T	13-10-2005
		US 2005246536 A1	03-11-2005
EP 1594122 A	09-11-2005	AUCUN	
US 7194620 B1	20-03-2007	AUCUN	
US 7020555 B1	28-03-2006	US 7089113 B1	08-08-2006
US 2002191809 A1	19-12-2002	US 2005097333 A1	05-05-2005
		US 2005097334 A1	05-05-2005