PCT ORGANISATION MONDIALE DE LA PROPRIETE INTELLECTUELLE
Bureau international

DEMANDE INTERNATIONALE PUBLIEE EN VERTU DU TRAITE DE COOPERATION EN MATIERE DE BREVETS (PCT)

(51) Classification internationale des brevets 7 :		(11) Numéro de publication internationale:
H04L 9/32	**A1**	**WO 00/02343**
		(43) Date de publication internationale: 13 janvier 2000 (13.01.00)

(21) Numéro de la demande internationale: PCT/CH99/00286

(22) Date de dépôt international: 1er juillet 1999 (01.07.99)

(30) Données relatives à la priorité:
1408/98 1er juillet 1998 (01.07.98) CH

(71) Déposant *(pour tous les Etats désignés sauf US)*: FASTCOM TECHNOLOGY S.A. [CH/CH]; PSE-B, CH-1015 Lausanne (CH).

(72) Inventeur; et
(75) Inventeur/Déposant *(US seulement)*: MOSCHENI, Fabrice [CH/CH]; Fastcom Technology S.A., PSE-B, CH-1015 Lausanne (CH).

(74) Mandataire: ROLAND, André; André Roland Intellectual Property Services, Case postale 1259, 38, rue du Petit-Chêne, CH-1001 Lausanne (CH).

(81) Etats désignés: AE, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, DE, DK, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, UA, UG, US, UZ, VN, YU, ZA, ZW, brevet ARIPO (GH, GM, KE, LS, MW, SD, SL, SZ, UG, ZW), brevet eurasien (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), brevet européen (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), brevet OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Publiée
Avec rapport de recherche internationale.
Avant l'expiration du délai prévu pour la modification des revendications, sera republiée si des modifications sont reçues.

(54) Title: METHOD FOR AUTHENTICATING AND VERIFYING DIGITAL DATA INTEGRITY

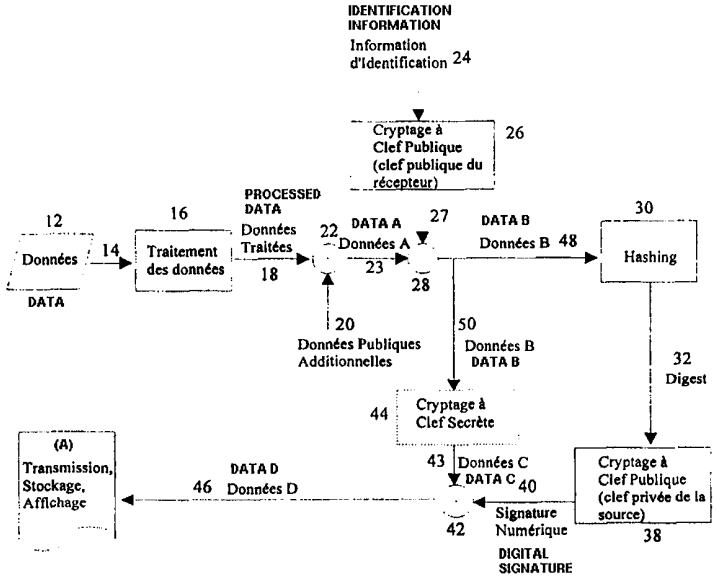
(54) Titre: METHODE D'AUTHENTIFICATION ET DE VERIFICATION DE L'INTEGRITE DE DONNEES NUMERIQUES

(57) Abstract

The invention concerns digital integrated systems which process data in real time. More precisely, it concerns a security technique which enables the digital data receiver to authenticate their source and integrity. The invention is characterised in that it consists in adding an encrypted identification information to the digital data to be transmitted.

(57) Abrégé

La présente invention se rapporte aux systèmes intégrés numériques qui traitent l'information en temps réel. Plus précisément, elle a trait à une technique de sécurité qui permet au récepteur de données numériques d'authentifier leur source et leur intégrité. Elle se caractérise notamment par le fait que l'on ajoute une information d'identification cryptée aux données numériques à transmettre.



(A) ... TRANSMISSION STORAGE DISPLAY
16 ... DATA PROCESSING
20 ... SUPPLEMENTARY PUBLIC DATA
44 ... SECRET KEY ENCRYPTION
26 ... PUBLIC KEY ENCRYPTION (RECEIVER PUBLIC KEY)
38 ... PUBLIC KEY ENCRYPTION (PRIVATE KEY OF SOURCE)

UNIQUEMENT A TITRE D'INFORMATION

Codes utilisés pour identifier les Etats parties au PCT, sur les pages de couverture des brochures publiant des demandes internationales en vertu du PCT.

AL	Albanie	**ES**	Espagne	**LS**	Lesotho	**SI**	Slovénie
AM	Arménie	**FI**	Finlande	**LT**	Lituanie	**SK**	Slovaquie
AT	Autriche	**FR**	France	**LU**	Luxembourg	**SN**	Sénégal
AU	Australie	**GA**	Gabon	**LV**	Lettonie	**SZ**	Swaziland
AZ	Azerbaïdjan	**GB**	Royaume-Uni	**MC**	Monaco	**TD**	Tchad
BA	Bosnie-Herzégovine	**GE**	Géorgie	**MD**	République de Moldova	**TG**	Togo
BB	Barbade	**GH**	Ghana	**MG**	Madagascar	**TJ**	Tadjikistan
BE	Belgique	**GN**	Guinée	**MK**	Ex-République yougoslave de Macédoine	**TM**	Turkménistan
BF	Burkina Faso	**GR**	Grèce			**TR**	Turquie
BG	Bulgarie	**HU**	Hongrie	**ML**	Mali	**TT**	Trinité-et-Tobago
BJ	Bénin	**IE**	Irlande	**MN**	Mongolie	**UA**	Ukraine
BR	Brésil	**IL**	Israël	**MR**	Mauritanie	**UG**	Ouganda
BY	Bélarus	**IS**	Islande	**MW**	Malawi	**US**	Etats-Unis d'Amérique
CA	Canada	**IT**	Italie	**MX**	Mexique	**UZ**	Ouzbékistan
CF	République centrafricaine	**JP**	Japon	**NE**	Niger	**VN**	Viet Nam
CG	Congo	**KE**	Kenya	**NL**	Pays-Bas	**YU**	Yougoslavie
CH	Suisse	**KG**	Kirghizistan	**NO**	Norvège	**ZW**	Zimbabwe
CI	Côte d'Ivoire	**KP**	République populaire démocratique de Corée	**NZ**	Nouvelle-Zélande		
CM	Cameroun			**PL**	Pologne		
CN	Chine	**KR**	République de Corée	**PT**	Portugal		
CU	Cuba	**KZ**	Kazakstan	**RO**	Roumanie		
CZ	République tchèque	**LC**	Sainte-Lucie	**RU**	Fédération de Russie		
DE	Allemagne	**LI**	Liechtenstein	**SD**	Soudan		
DK	Danemark	**LK**	Sri Lanka	**SE**	Suède		
EE	Estonie	**LR**	Libéria	**SG**	Singapour		

Méthode d'authentification et de vérification de l'intégrité de données numériques

Domaine de l'invention

La présente invention se rapporte aux systèmes intégrés numériques qui traitent l'information en temps réel.

Plus précisément, elle a trait à une technique de sécurité qui permet au récepteur de données numériques d'authentifier leur source et leur intégrité.

Etat de la technique

L'authentification de la source de données numériques, telles qu'images, séquences d'images ou son, est généralement faite dans un but de copyright. L'objectif est de cacher dans les données une information d'identification de la source et ceci de façon invisible (par ex. les techniques de « watermarking »). Une telle authentification protège les données contre des usages illicites car les données contiennent l'information permettant d'authentifier le propriétaire du copyright. Des exemples de cette fonctionnalité sont décrits dans le brevet US-A-5 668 603 et le brevet US-A-5 636 292.

La vérification de l'intégrité des données numériques est communément utilisée dans des applications de réseaux. Le but est de certifier que les données numériques sont originales et n'ont pas été corrompues pendant la transmission. La vérification de l'intégrité est généralement effectuée grâce à une signature numérique. La signature numérique est générée par cryptage d'un «digest» des données numériques dont l'intégrité doit être vérifiée. Le digest des données est obtenu par «hashing» de ces dernières. Le hashing est une transformation mathématique qui, à partir de données de longueur arbitraire, calcule un nombre de longueur fixe. Le cryptage du digest se fait généralement avec un schéma à clef publique. Un tel schéma de cryptage est également appelé schéma de cryptage asymétrique. La signature numérique permet d'authentifier la source des données numériques car la source est la seule à connaître la clef privée du schéma. De plus, la signature numérique permet de vérifier l'intégrité des données numériques. Un exemple de cette fonctionnalité est décrit dans: Massachusetts Institute of Technology, document MIT/LCS/TM-82, "A Method for Obtaining Digital Signatures in Public-Key Cryptosystems", écrit par Rivest et al. Les

schémas de cryptage à clef publique sont notamment décrits dans le brevet US-A-4 405 829. L'autre grande classe de schémas de cryptage sont ceux à clef secrète. Un tel schéma de cryptage est également appelé schéma de cryptage symétrique. Référence est donnée au standard «Data Encryption Standard (DES)», FIPS PUB 46, National Bureau of Standards, U.S. Department of Commerce, Washington, DC, janvier 1997. Finalement, en ce qui concerne le «hashing», référence est donnée à R. Rivest, "The MD5 Message Digest Algorithm", RFC 1321, avril 1992.

La demande de brevet EP-A-689 316 présente une méthode de cryptage à schéma symétrique utilisée avec des réseaux sans fil. Chaque message envoyé est constitué de trois segments : Le premier contenant une information d'identification non cryptée, le ESN, le deuxième contenant le paquet de données à transmettre (information utile) et le troisième contenant une signature numérique qui est obtenue par application d'un algorithme de "hashing" et un algorithme de cryptage au paquet de données à transmettre.

Les méthodes de l'état de la technique, bien qu'elles offrent une certaine sécurité, présentent cependant un certain nombre de faiblesses.
Par exemple, lorsque l'information d'identification n'est pas cryptée, une personne mal intentionnée peut parfaitement déterminer la provenance du paquet de données, de pratiquer des analyses statistiques sur ces dernières et, sans trop d'effort, en déduire les clés de cryptage du paquet de données.

Résumé de l'invention

Un des objets de la présente invention vise a améliorer la sécurité liée à la transmission, au stockage ou à la visualisation de données numériques et plus particulièrement lorsqu'il s'agit de données audiovisuelles.
Cet objectif est atteint en utilisant une technique de sécurité qui permet au récepteur de données numériques, d'une part, d'authentifier de façon univoque la source des données grâce à une information d'identification, unique et cryptée, qui est ajoutée aux données numériques, et d'autre part, de vérifier l'intégrité des données numériques. Si nécessaire, la technique permet également d'assurer le secret des données. L'information d'identification cryptée de la source authentifie de façon univoque la source des données numériques.

Chaque source possède son code d'identification, nommé ci-après « ID code », qui est unique et stocké localement dans son hardware et dans une mémoire uniquement lisible (mémoire ROM). Le code ID est la base de l'information d'identification. L'information d'identification peut également contenir des informations additionnelles telles que l'heure, la date de la capture et la location de la source.

La source peut générer différents types de données numériques, la liste non-exhaustive suivante en donne quelques exemples :

- Son, image ou séquence d'image
- Résultats de traitements de signal effectués sur des données sonores, visuelles ou audiovisuelles
- Signaux utilisés par la source pour interagir avec d'autres équipements avec lesquels la source est connectée et/ou interagit (par ex. signal de la source pour commander le mécanisme d'ouverture d'une porte).

Dans le texte qui suit, on décrira essentiellement des données audiovisuelles numériques, à transmettre ou à stocker ou à visualiser, traitées ou non par des méthodes de traitement du signal. On peut imaginer que ces données soient complétées par des données publiques additionnelles. L'ensemble de ces données sera simplement nommée «les données» ou «données à transmettre». La source de ces données sera dénommée «la source».

La procédure qui rend possible l'authentification de la source, la vérification de l'intégrité des données et le cryptage des données est menée à bien au niveau de la source elle-même, avant toute transmission, tout stockage ou affichage des données. Le récepteur effectue l'authentification de la source, la vérification de l'intégrité des données et le décryptage des données après les avoir reçues.

La procédure rendant possible l'authentification sécurisée de la source consiste à crypter l'information d'identification de la source et de l'ajouter aux données à transmettre. Le cryptage de l'information d'identification peut se faire soit par un système symétrique, soit par un système asymétrique.

L'ajout de l'information d'identification cryptée se fait soit par concaténation de l'information d'identification cryptée aux données à transmettre, soit par insertion visible ou

invisible de l'information d'identification cryptée (p.ex. techniques de watermarking, ...) dans les données elles-mêmes, soit en faisant parallèlement une concaténation aux données à transmettre et une insertion dans ces mêmes données à transmettre.

Dans le cas où une insertion de l'information d'identification cryptée dans les données à transmettre est effectuée, les données à transmettre seront modifiées. Dans ce cas, ce sont ces données modifiées qui seront utilisées en lieu est place des données originales. Dans le reste du texte, on les nommera néanmoins «les données».

Puis, les données sont utilisées pour générer une signature numérique dans le cadre d'un schéma standard de signature numérique. La signature numérique est ajoutée aux données à transmettre par concaténation.

Dans le cas où la confidentialité des données serait désirée, les données sont cryptées avant la transmission. Après cette étape optionnelle de cryptage, des données publiques additionnelles peuvent être ajoutées aux données à transmettre.

Si les données sont corrompues avant que le récepteur ne les reçoive, l'authentification de la source et/ou la vérification de l'intégrité des données ne sera pas possible. Le récepteur ne pourra donc pas certifier l'origine des données et/ou leur intégrité.

L'authentification sécurisée de la source est basée sur le ID code unique à chaque source et non pas sur le schéma de cryptage à clef publique. En effet, le cryptage de l'information d'identification dans laquelle se trouve l'ID code peut se faire grâce à un schéma de cryptage à clef publique qui utilise une clef définie par software, facilement modifiable, et qui n'est pas nécessairement unique à chaque source, car pouvant être partagée entre plusieurs sources. A l'opposé, le ID code, stocké de manière indélébile dans le hardware de la source, ne peut être modifié sans endommager la source et, par définition, est unique à chaque source. Ces caractéristiques permettent de suivre chaque source à travers tout le temps de son utilisation.

De plus, l'invention ne limite pas le type de schémas de cryptage et/ou de clefs utilisés pour le cryptage de l'information d'identification.

L'invention ne se veut pas robuste contre les tentatives de malversation des données après que ces dernières ont quitté la source. Au contraire, les fonctionnalités permises par l'invention disparaissent en partie ou totalement en cas de malversation, ce qui permet au récepteur de détecter la fraude.

La présente invention trouve donc plusieurs domaines d'applications, notamment:

- Surveillance vidéo de sécurité
- Génération de données ayant valeur de preuves légales
- Recherche automatique d'événements dans une base de données audiovisuelles
- Contrôle d'équipements d'un réseau limité à la source audiovisuelle

Un mode de réalisation de l'invention est décrit ci-après au moyen des figures suivantes:

Figure 1: Ajout de l'information d'identification et de données publiques additionnelles au niveau de la source de données telle que décrit dans l'état de la technique.

Figure 2: Préparation du paquet d'information à transmettre au niveau de la source

Figure 3: Traitement du paquet d'information reçu au niveau du récepteur

Pour ce mode de réalisation de l'invention, on se place dans le cas d'une source décentralisée de données audiovisuelles numériques. Les données sont envoyées au récepteur soit «on-line» soit «off-line».

Dans la description de la réalisation de l'invention, lorsque nous parlons d'«ajout» ou d'«ajouter» des informations dans les données, cela peut se faire soit d'une manière invisible en insérant l'information dans les données même (par ex. watermarking), soit d'une manière visible en concaténant les informations et les données dans un seul et même paquet. Dans ce dernier cas, le protocole de concaténation est à définir.

Dans la description de la réalisation de l'invention, lorsque nous parlons de «séparation» ou de «séparer» des données en ses composants, cela correspond au processus inverse du processus «ajout» décrit ci-dessus. Lorsque nous parlons d'«extraction» d'information depuis

les données, cela correspond à une extension du processus de «séparation» défini ci-dessus, où d'un paquet de données formé de plus de deux composants, seul un est extrait du paquet.

Dans les figures, le symbole ⊗ signifie «ajout», alors que le symbole ◯ signifie selon les cas soit «séparation», soit «extraction».

Dans la réalisation non-sure et tronquée de l'état de la technique telle qu'illustrée à la Figure 1, les Données (12) sont en premier lieu traitées, ce qui produit les Données Traitées (18). Les traitements de données possibles incluent des opérations telles que compression avec ou sans pertes qui visent à réduire la taille des données ou des schémas d'analyse des données qui visent à extraire des données les informations significatives. Des Données Publiques Additionnelles (20) sont ensuite ajoutées (22) aux Données Traitées (18), les données résultantes étant les Données A (23). Les Données Publiques Additionnelles (20) sont typiquement les paramètres utilisés pour traiter les Données (12), par ex. paramètres de codage. L'Information d'Identification (24) est ajoutée (28) aux Données A, ce qui donne naissance aux Données D 46. Ces dernières peuvent ensuite être transmises, stockées ou affichées. Malgré le fait que le système décrit dans la Figure 1 soit censé authentifier de façon univoque la source des données grâce à l'Information d'Identification (24), le système ne permet pas de détecter si un individu malintentionné a modifié les Données D 46, pouvant provoquer ainsi une fausse identification de la source.

Le mode de réalisation de l'invention présenté aux Figures 2 et 3 remédie aux problèmes illustrés plus haut. La Figure 2 décrit la réalisation de l'invention au niveau de la source des données. La Figure 3 décrit la réalisation de l'invention au niveau du récepteur des données. Nous supposons que la source possède une paire de clefs publique/privée d'un schéma de cryptage à clef publique. Nous faisons la même hypothèse pour le récepteur des données. De plus, nous supposons que la source et le récipient partage la clef secrète d'un schéma de cryptage à clef secrète. La clef peut être changée dynamiquement au cours du temps.

Au niveau de la source (voir Figure 2), les Données (12) sont en premier lieu traitées 16 pour donner lieu aux Données Traitées (18). Les possibles traitements des données incluent des opérations telles que compression avec ou sans perte et analyses des données pour en extraire les informations désirées. Les Données Publiques Additionnelles (20) sont ensuite ajoutées (22) aux Données Traitées, ceci donnant lieu aux Données A 23. Les Données Publiques Additionnelles (22) sont typiquement les informations telles que les paramètres utilisés pour traiter les Données (12), e.g. paramètres de compression. L'Information d'Identification (24)

est ajoutée (28) aux Données A 23 donnant lieu aux Données B 48. Un Cryptage à Clef Publique (26) est accompli sur l'Information d'Identification avant de l'ajouter aux Données A 23. Le Cryptage à Clef Publique (26) est accompli en utilisant la clef publique du récepteur. La Signature Numérique (40) est générée à partir des Données B 48. A cette fin, un hashing (30) des Données B 48 est effectué pour obtenir le Digest (32). Ensuite, la Signature Numérique (40) est obtenue grâce au Cryptage à Clef Publique (38) du Digest (32). Le Cryptage à Clef Publique (38) est effectué en utilisant la clef privée de la source. La Signature Numérique (40) est alors ajoutée (42) aux Données C 43, ceci donnant lieu aux Données D 46. Les Données C 43 sont le résultat du cryptage optionnel par Cryptage à Clef Secrète (44) des Données B 50 (les Données B 50 et les Données B 48 sont identiques). L'option du Cryptage à Clef Secrète (44) permet d'assurer le secret des Données B 50 si nécessaire. Dans le cas où le Cryptage à Clef Secrète (44) n'est pas effectué, les Données B 50 et les Données C 43 sont identiques.

Au niveau du récepteur (voir Figure 3), les données reçues, les Données D 82, sont séparées (88) en leurs deux composants qui sont les Données C 86 et la Signature Numérique (90). La Signature Numérique permet au récepteur de Vérifier l'Intégrité (98) des Données D 82. La Signature Numérique (90) est décryptée par le schéma de Décryptage à Clef Publique (92) qui utilise la clef publique de la source. Le Décryptage à Clef Publique (92) permet d'obtenir le Digest (94), qui est le digest original généré dans la source. Pour vérifier l'intégrité des Données D 82, le récepteur compare (96) le Digest (94) avec le résultat (104) du Hashing (102) des Données B 101. Le résultat (97) de la Comparaison (96) permet de dire si les données sont intègres ou non (98).

Les Données B 100 (les Données B 100 et les Données B 101 sont identiques) résultent du Décryptage à Clef Secrète (84) des Données C 86. Le Décryptage à Clef Secrète (84) est nécessaire au cas où les Données B 50 ont été cryptées (44) au niveau de la source (voir Figure 2). Le décryptage utilise la clef secrète du schéma de cryptage à clef secrète. Cette clef secrète est un secret partagé entre la source et le récepteur. Ceci garantit la confidentialité des Données C 86. Au cas où le cryptage (44) n'aurait pas été effectué, les Données C 86 et les Données B 100 sont identiques.

Les Données B 100 sont utilisées pour l'Authentification (126) de la source. Les Données B (100) contiennent également les Données Publiques Additionnelles (112) et les Données Traitées (114). Pour authentifier la source (126), l'Information d'Identification (120) est extraite (106) des Données B 100. L'Information d'Identification (120) est décryptée par le schéma de Décryptage à Clef Publique (122) qui utilise la clef privée du récepteur,

l'Information d'Identification (124) ainsi obtenue étant alors utilisée par le récepteur pour Authentifier la Source (126) des Données D 82. En particulier, le ID code unique à chaque source est obtenu.

Après l'extraction (106) de l'Information d'Identification (120), les données restantes, les Données A (108), ont deux composants qui sont les Données Publiques Additionnelles (112) et les Données Traitées (114). Ces deux composants sont séparés (110) et rendus disponibles au récepteur.

La réalisation de l'invention décrite ci-dessus présente les fonctionnalités de confidentialité des données, de vérification de l'intégrité des données et d'authentification de la source des données. Cette méthode est fragile. Toute tentative de modifier les données durant leur transmission, leur stockage ou avant leur affichage est détectée. La réalisation de l'invention décrite ci-dessus est illustrative et n'est pas limitative.

Revendications

1. Méthode, applicable aux systèmes intégrés numériques qui traitent l'information en temps réel, pour authentifier la source de façon sécurisée et pour vérifier l'intégrité et la confidentialité des données numériques reçues par le récepteur, caractérisée par le fait qu'au niveau de la source, elle comprend les étapes suivantes :
   - Cryptage d'une information d'identification dont la base est un ID code, unique à chaque source et stocké en hardware localement dans la source, le ID code est stocké dans une mémoire de type ROM de la source même; en sus de l'ID code, l'information d'identification peut également contenir des informations additionnelles telles que date, heure et location de la source
   - Génération d'une signature numérique des données numériques; la signature numérique est obtenue par cryptage du digest des données numériques, le digest étant obtenu grâce à un «hashing» des données numériques et le cryptage pouvant être effectué par une méthode de cryptage symétrique ou une méthode de cryptage asymétrique
   - Cryptage optionnel du paquet de données numériques
   - Ajout optionnel de données publiques aux données numériques
   - Génération et transmission du paquet formé par concaténation de l'information d'identification cryptée, les données numériques et la signature numérique.

2. Méthode selon la revendication 1, caractérisée par le fait que l'information d'identification cryptée est ajoutée par insertion visible ou invisible dans les données numériques.

3. Méthode selon la revendication 2, caractérisée par le fait que le paquet généré et transmis n'est formé que par la concaténation des données numériques et de la signature numérique.

4. Méthode selon l'une des quelconques revendications précédentes, caractérisée par le fait que des données publiques additionnelles complètent les données numériques.

5. Méthode selon l'une des quelconques revendications précédentes, caractérisée par le fait que les données à transmettre sont le résultat de méthodes de traitement de signal effectuées sur des signaux numériques capturés par la source ou présents dans la source.

6. Méthode selon l'une des quelconques revendications précédentes, caractérisée par le fait que la ou les clés utilisée(s) pour le cryptage est/sont indépendante(s) de l'information d'identification.

7. Méthode selon l'une quelconque des revendications précédentes, caractérisée par le fait que l'information d'identification est cryptée avec une ou des clés qui correspondent au type de traitement de signal appliqué aux données numériques avant leur transmission.

8. Méthode selon l'une des quelconques revendications précédentes, caractérisée par le fait que l'information d'identification est cryptée avec une ou des méthodes de cryptage qui correspondent au type de traitement de signal appliqué aux données numériques avant leur transmission.

9. Méthode selon l'une quelconque des revendications précédentes, caractérisée par le fait le cryptage de l'information de d'identification s'effectue selon un schéma asymétrique.

10. Méthode selon l'une quelconque des revendications précédentes, caractérisée par le fait qu'elle s'applique aux systèmes vidéo qui comprennent au moins une caméra intelligente.

11. Méthode selon l'une quelconque des revendications précédentes, caractérisée par le fait qu'au niveau du récepteur, elle comprend au moins les étapes suivantes au cas où l'information d'identification cryptée aurait été insérée dans les données numériques:
    - Séparation des données et de la signature numérique
    - Séparation des données numériques et de l'information d'identification cryptée
    - Décryptage et extraction de l'information d'identification
    - Authentification de la source des données

12. Méthode selon l'une quelconque des revendications précédentes, caractérisée par le fait qu'au niveau du récepteur, elle comprend au moins les étapes suivantes au cas où l'information d'identification cryptée aurait été concaténée aux données numériques:
    - Séparation de l'information d'identification cryptée, des données et de la signature numérique
    - Décryptage et extraction de l'information d'identification
    - Authentification de la source des données

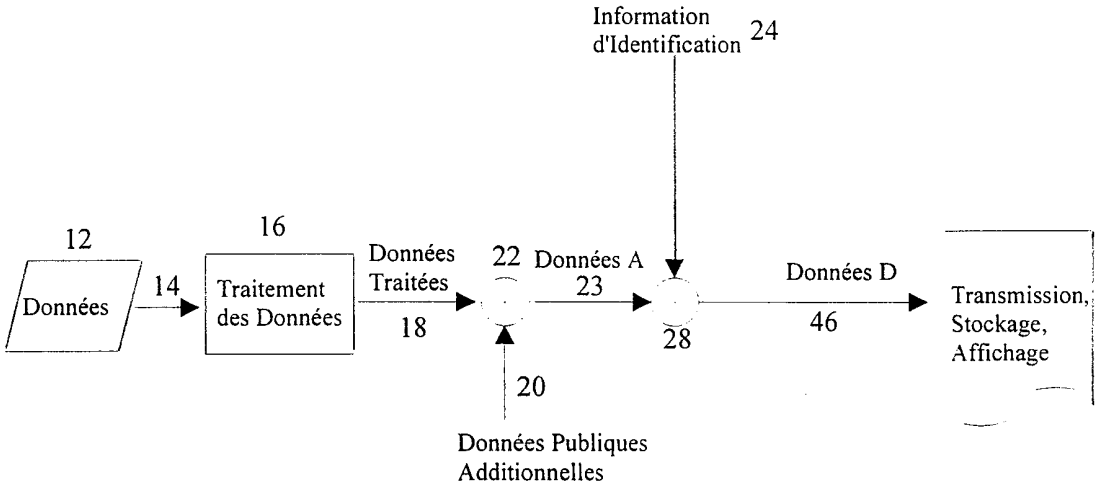

Information
d'Identification
24
12
Données
14
16
Traitement
des Données
Données
Traitées
18
22
Données A
23
28
Données D
46
Transmission,
Stockage,
Affichage
20
Données Publiques
Additionnelles

Fig. 1

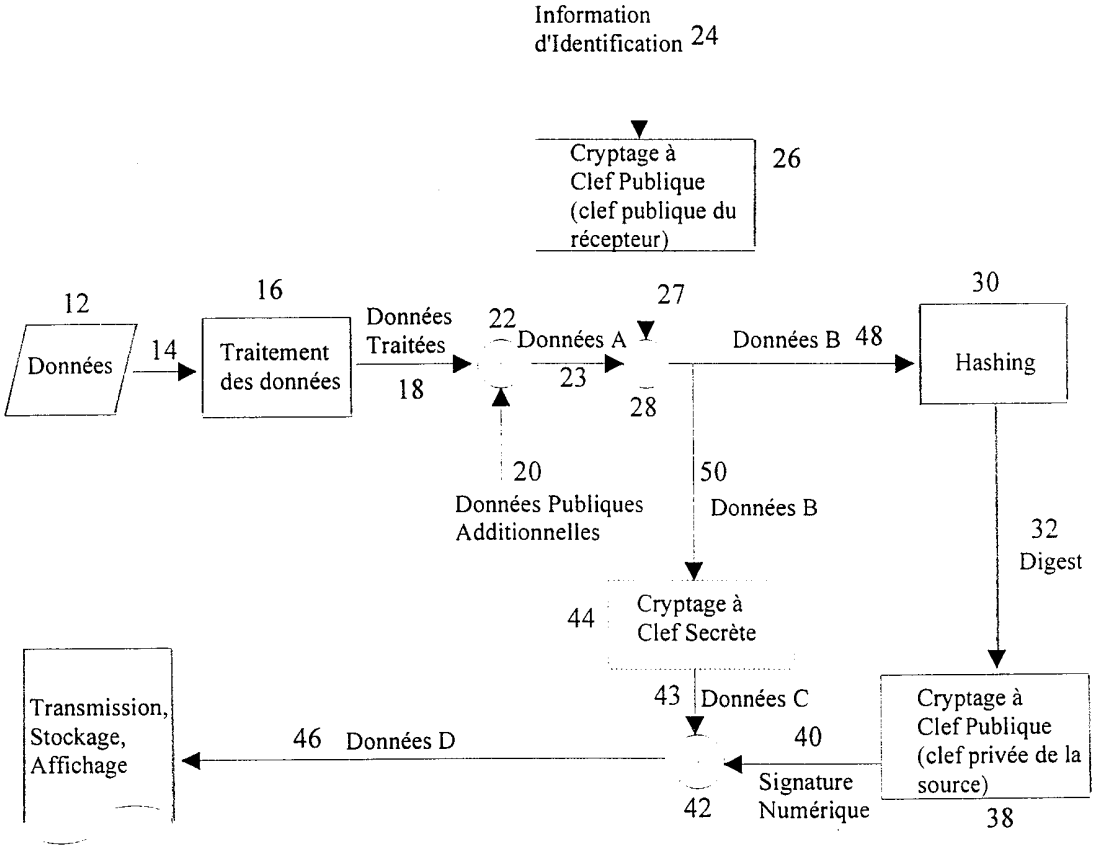

Information d'Identification 24
Cryptage à Clef Publique (clef publique du récepteur)
26
12
Données
14
16
Traitement des données
Données Traitées
18
22
Données A
23
27
28
Données B 48
30
Hashing
20
Données Publiques Additionnelles
50
Données B
32
Digest
44
Cryptage à Clef Secrète
43
Données C
40
Signature Numérique
42
Cryptage à Clef Publique (clef privée de la source)
38
46 Données D
Transmission, Stockage, Affichage

Fig. 2

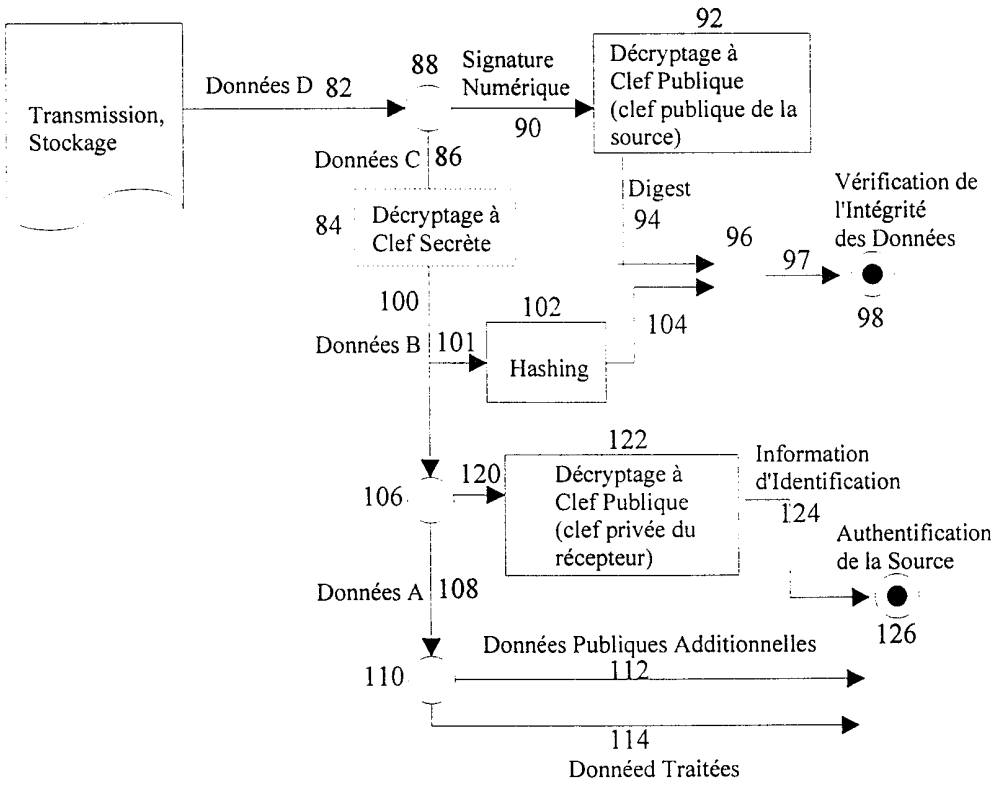

Transmission, Stockage
Données D 82
88
Signature Numérique
90
92
Décryptage à Clef Publique (clef publique de la source)
Données C 86
84
Décryptage à Clef Secrète
Digest
94
96
97
Vérification de l'Intégrité des Données
98
100
102
Données B 101
Hashing
104
122
106
120
Décryptage à Clef Publique (clef privée du récepteur)
Information d'Identification
124
Authentification de la Source
126
Données A 108
Données Publiques Additionnelles
112
110
114
Donnéed Traitées

Fig. 3

INTERNATIONAL SEARCH REPORT

Inter onal Application No
PCT/CH 99/00286

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 H04L9/32

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)
IPC 7 H04L

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)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	WO 98 00972 A (SUN MICROSYSTEMS INC) 8 January 1998 (1998-01-08) page 11, paragraph 3 -page 13, line 7 ---	1,9,11
A	US 5 499 294 A (FRIEDMAN GARY L) 12 March 1996 (1996-03-12) abstract column 4, line 55 -column 5, line 8 column 5, line 49 -column 6, line 14 column 7, line 6 - line 19 column 9, line 8 - line 28 ---	1,10
A	EP 0 689 316 A (AT & T CORP) 27 December 1995 (1995-12-27) cited in the application column 3, line 53 -column 7, line 7 --- -/--	1,3

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in 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
25 October 1999	05/11/1999

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, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Holper, G

1

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Inter' 'onal Application No
PCT/CH 99/00286

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication,where appropriate, of the relevant passages	Relevant to claim No.
A	KIYOSHI TANAKA ET AL: "A DIGITAL SIGNATURE SCHEME ON A DOCUMENT FOR MH FACSIMILE TRANSMISSION" ELECTRONICS & COMMUNICATIONS IN JAPAN, PART I - COMMUNICATIONS, vol. 74, no. 8, 1 August 1991 (1991-08-01), pages 30-36, XP000287493 ISSN: 8756-6621 page 31, right-hand column, last paragraph -page 32, left-hand column, paragraph 1	1,2

1

INTERNATIONAL SEARCH REPORT

.formation on patent family members

Interr ·nal Application No
PCT/CH 99/00286

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 9800972 A	08-01-1998	US 5825884 A	20-10-1998
		EP 0847649 A	17-06-1998
US 5499294 A	12-03-1996	NONE	
EP 0689316 A	27-12-1995	CA 2149067 A	23-12-1995
		JP 8032575 A	02-02-1996

RAPPORT DE RECHERCHE INTERNATIONALE

Demande internationale No
PCT/CH 99/00286

A. CLASSEMENT DE L'OBJET DE LA DEMANDE
CIB 7 H04L9/32

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)
CIB 7 H04L

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 réalisable, termes de recherche utilisés)

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 98 00972 A (SUN MICROSYSTEMS INC) 8 janvier 1998 (1998-01-08) page 11, alinéa 3 -page 13, ligne 7 ---	1,9,11
A	US 5 499 294 A (FRIEDMAN GARY L) 12 mars 1996 (1996-03-12) abrégé colonne 4, ligne 55 -colonne 5, ligne 8 colonne 5, ligne 49 -colonne 6, ligne 14 colonne 7, ligne 6 - ligne 19 colonne 9, ligne 8 - ligne 28 ---	1,10
A	EP 0 689 316 A (AT & T CORP) 27 décembre 1995 (1995-12-27) cité dans la demande colonne 3, ligne 53 -colonne 7, ligne 7 --- -/--	1,3

[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'appartenant 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
25 octobre 1999	05/11/1999

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, Tx. 31 651 epo nl, Fax: (+31–70) 340–3016	Holper, G

1

RAPPORT DE RECHERCHE INTERNATIONALE

Dem 'e internationale No
PCT/CH 99/00286

C.(suite) DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie °	Identification des documents cités, avec,le cas échéant, l'indicationdes passages pertinents	no. des revendications visées
A	KIYOSHI TANAKA ET AL: "A DIGITAL SIGNATURE SCHEME ON A DOCUMENT FOR MH FACSIMILE TRANSMISSION" ELECTRONICS & COMMUNICATIONS IN JAPAN, PART I - COMMUNICATIONS, vol. 74, no. 8, 1 août 1991 (1991-08-01), pages 30-36, XP000287493 ISSN: 8756-6621 page 31, colonne de droite, dernier alinéa -page 32, colonne de gauche, alinéa 1	1,2

1

RAPPORT DE RECHERCHE INTERNATIONALE

Renseignements relatifs . . membres de familles de brevets

Dem 'e internationale No
PCT/CH 99/00286

Document brevet cité au rapport de recherche	Date de publication	Membre(s) de la famille de brevet(s)	Date de publication
WO 9800972 A	08-01-1998	US 5825884 A	20-10-1998
		EP 0847649 A	17-06-1998
US 5499294 A	12-03-1996	AUCUN	
EP 0689316 A	27-12-1995	CA 2149067 A	23-12-1995
		JP 8032575 A	02-02-1996