(19) RÉPUBLIQUE FRANÇAISE

INSTITUT NATIONAL
DE LA PROPRIÉTÉ INDUSTRIELLE

PARIS

(11) **N° de publication :** **2 820 843**
(à n'utiliser que pour les commandes de reproduction)

(21) **N° d'enregistrement national :** **01 01808**

(51) Int Cl[7] : **G 06 F 9/44,** G 06 K 19/06, G 11 B 7/00

(12) DEMANDE DE BREVET D'INVENTION A1

(22) **Date de dépôt :** 09.02.01.

(30) **Priorité :**

(43) **Date de mise à la disposition du public de la demande :** 16.08.02 Bulletin 02/33.

(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) :** *THOMSON CSF Société anonyme* — FR et *MOULAGE PLASTIQUE DE L'OUEST* — FR.

(72) **Inventeur(s) :** RIGUIDEL MICHEL et BEUZIT THIERRY.

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

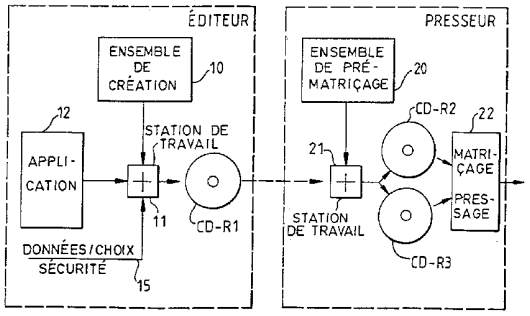
(74) **Mandataire(s) :** THALES "INTELLECTUAL PROPERTY".

(54) SYSTEME DE PROTECTION CONTRE LA COPIE D'INFORMATIONS POUR LA CREATION D'UN DISQUE OPTIQUE PROTEGE ET PROCEDE DE PROTECTION CORRESPONDANT.

(57) L'invention concerne un système de protection contre la copie d'informations pour la création d'un disque optique protégé.

Le système comprend, chez l'éditeur d'une application (12), un ensemble logiciel de création (10) porté par un disque optique auto-protégé comprenant un ensemble d'éléments de protection permettant à l'éditeur d'insérer dans l'application un fichier de protection traduisant ses choix stratégiques de protection. L'ensemble résultant est transcrit sur un disque de transport (CD-R1) pour être envoyé chez le duplicateur. Celui-ci, à l'aide d'un ensemble logiciel de pré-matriçage (20) reconstruit le contenu du disque définitif comportant une zone de protection en deux parties, sous la forme de deux disques (CD-R2, CD-R3) contenant respectivement les données de la piste principale avec la première partie de la zone de protection et de la seconde partie.

L'invention s'applique à la création de disques optiques protégés contre la copie.



FR 2 820 843 - A1

La présente invention se rapporte à un système de protection contre la copie d'informations pour la création d'un disque optique protégé du type comportant au moins une piste principale en spirale et une zone de protection à deux parties de même taille dont une au moins appartient à la piste principale. Elle se rapporte également à un procédé de protection correspondant.

De nombreuses techniques ont été développées, en particulier ces dernières années, pour empêcher la copie illégale des disques optiques. Une des plus simples parmi celles-ci consiste à inscrire en un endroit prédéterminé du disque, lors de sa fabrication, un code de protection contre la copie. Cet endroit prédéterminé est tel que de nombreuses techniques de copie ne peuvent pas reproduire cet endroit du disque. Les lecteurs sont faits pour rejeter les disques n'ayant pas de code de protection au bon endroit. Mais il est évident que tout dispositif fait ou modifié pour lire toutes les données d'un disque peut copier le disque y compris son code de protection, et la copie illégale obtenue est exactement semblable au disque original.

Une autre technique connue est la méthode SCMS (« Serial Copy Management System ») selon laquelle un disque porte un code SCMS qui autorise ou non la copie. Un disque ayant un code SCMS autorisant la copie peut être copié mais le dispositif de copie change le code SCMS pour un code interdisant toute autre copie. Mais, comme on le voit, cette technique souffre du même inconvénient que précédemment lorsque l'on copie toutes les données du disque telles quelles.

D'autres techniques relativement sophistiquées ont été imaginées pour remédier aux problèmes de copie non autorisées. La plupart d'entre elles impliquent l'utilisation d'une «signature » ou empreinte spécifique sur le disque. Cela peut consister en une variation de certains paramètres de gravure sur le disque, tels que forme des marques (profondeur, largeur, longueur), introduction d'une asymétrie des marques, wobulation de la piste à des fréquences particulières, etc... Ces variations constituent la signature à

rechercher et ne peuvent être reproduites par des graveurs usuels tels que les graveurs de CD-R. Cependant, il est nécessaire que les lecteurs de disque détectent ces variations et cela n'est généralement pas possible avec des lecteurs standards. Une variante de cette méthode permet de créer des mots de code ambigus susceptibles d'être lus avec des valeurs différentes lors de plusieurs lectures successives du disque avec des lecteurs standards.

Une technique différente consiste à détruire ou endommager volontairement des spires ou secteurs du disque original dont les adresses peuvent être cryptées pour constituer un code identificateur du disque inscrit sur celui-ci. Cependant, un inconvénient de ce genre de technique est qu'elle nécessite d'authentifier l'utilisateur du disque par une information d'accès plus ou moins complexe que l'utilisateur devra introduire comme clé pour obtenir l'accès au contenu du disque. Cette information doit souvent être demandée à une station d'habilitation. Cette technique impose donc des contraintes non négligeables. Un autre inconvénient de telles méthodes de reconnaissance de parties endommagées est qu'elle ne permet de cacher qu'une faible quantité de données, donc susceptible d'être aisément incorporée dans le corps du logiciel. Un autre inconvénient est que l'écriture de telles marques est structurellement à la portée des graveurs de disques du commerce, le seul obstacle à la recopie des disques étant que le logiciel de commande de ces graveurs est inadapté à la gestion de telles marques, erreurs ou omissions. Une modification de l'un des logiciels de commande (au niveau du processeur utilisateur ou du logiciel interne du graveur) serait cependant suffisante pour recopier ces disques. On peut noter ici que l'endommagement du disque peut à la limite consister en l'omission pure et simple de certains secteurs.

Pour essayer de remédier à certains de ces inconvénients et renforcer la sécurité des systèmes antipiratage à codes cachés, on a développé des techniques à spirale interrompue ou à zones séparées entre lesquelles les données sont réparties de façon à interdire un enregistrement en continu de données exécutables. De telles techniques peuvent toutefois entraîner une réduction de densité des informations sur le disque ou parfois l'utilisation de lecteurs non-standards.

Une voie paraissant plus prometteuse a été esquissée en prévoyant un disque comportant une spirale ou piste principale continue entre les tours de laquelle est intercalé un tronçon de spirale secondaire, l'écartement ou pas standard des pistes de disque optique conventionnel étant conservé. Une méthode d'authentification consiste alors à « reconnaître » la spirale secondaire seulement en vérifiant la présence de codes d'identification ou d'adresses spécifiques qui ne se retrouvent pas sur la piste principale. Cependant cette technique ne met pas à profit de manière efficace l'intérêt majeur de disposer d'une zone qui n'est pas reproductible facilement par un graveur standard.

On a proposé récemment de remédier à ces inconvénients et de mettre à profit l'intérêt de l'existence d'une telle zone qui permet d'éliminer les copies classiques à l'aide de graveurs standard, grâce à la reconnaissance de la présence physique d'une zone de protection en deux parties.

Cette solution particulièrement intéressante prévoit un disque optique protégé contre la copie du type comportant au moins une piste principale en spirale sur laquelle sont inscrites des marques d'information rangées dans des secteurs dont les adresses sont sensiblement séquentielles le long de la piste, et une zone de protection à deux parties de même taille incluant chacune une série de secteurs désignés par des adresses identiques pour chaque partie, les informations stockées dans cette zone étant distribuées entre les secteurs des deux parties et chaque secteur de la zone portant en outre une information d'identification caractéristique de la partie à laquelle appartient le secteur, l'une des parties au moins appartenant à la piste principale.

Un sous-programme de protection permet de contrôler la présence et la constitution de ladite zone de protection et d'utiliser les informations stockées dans cette zone, les éléments d'informations dudit sous-programme étant enregistrés sur le disque.

L'avantage de l'existence d'une zone de protection en deux parties est particulièrement important si l'une des parties est disposée sur une piste secondaire intercalée partiellement entre des spires de la piste principale. Car ainsi, il devient impossible pour un graveur standard de réaliser un disque à deux pistes et on peut rendre très difficile toute copie

illégale d'un disque en vérifiant la structure physique du disque lu. De plus, même une modification de l'électronique de commande d'un équipement industriel de fabrication de disques-maîtres ne permettrait alors pas de dupliquer ces disques.

Pour améliorer encore la protection contre la copie, l'invention a pour but de mettre à profit les modifications physiques du disque mentionné ci-dessus en y ajoutant une partie logicielle permettant à une application cliente d'utiliser au mieux ces modifications physiques en compliquant grandement le travail d'un pirate et en rendant nécessaire de renouveler pratiquement tout ce travail de contournement pour chaque titre.

L'invention concerne donc un système pour la création d'un tel disque protégé et est caractérisée en ce que ce système comprend :

- un ensemble logiciel de création de protection pour permettre la création, chez l'éditeur d'une application destinée à être portée par ledit disque, d'un fichier de protection à partir d'éléments de protection dudit ensemble logiciel sélectionnés par l'éditeur et de données et paramètres choisis par l'éditeur ;
- un moyen de transport comportant ladite application et ledit fichier de protection ainsi que la localisation des fichiers correspondants sur le disque protégé, selon une arborescence déterminée par l'éditeur ;
- un ensemble logiciel de pré-matriçage pour, chez le duplicateur de disques et à partir des informations contenues dans ledit moyen de transport, déterminer et générer le contenu des deux parties dudit disque protégé ; et
- des moyens de stockage respectivement des informations de la piste principale, avec la première partie de la zone de protection, et de la seconde partie de cette zone pour la réalisation par le duplicateur des opérations ultérieures de matriçage et duplication du disque protégé.

Grâce à ce système mettant en œuvre un certain nombre d'éléments de protection logiciels évolutifs, on empêche la production d'un patch (« rustine », « adaptation » logicielle en français, mais le mot « patch » est généralement utilisé dans les milieux spécialisés et sera donc employé dans la suite) générique et on complique l'analyse et la compréhension de la

protection mise en œuvre. D'autres caractéristiques de l'invention sont définies dans la suite de la description.

Selon un autre aspect de l'invention, il est prévu un procédé de protection contre la copie d'informations enregistrées sur un disque optique protégé du type comportant au moins une piste principale en spirale, sur laquelle sont inscrites des marques d'information rangées dans des secteurs dont les adresses sont sensiblement séquentielles le long de la piste, et une zone de protection à deux parties sensiblement de même taille incluant chacune une série de secteurs désignés par des adresses identiques pour chaque partie, chaque secteur de la zone de protection incluant une information d'identification caractéristique de la partie à laquelle il appartient et l'une des parties au moins appartenant à ladite piste principale, ledit procédé étant caractérisé en ce qu'il consiste à créer un fichier de protection à partir d'éléments de protection logicielle sélectionnés lors de la création dudit fichier et à enregistrer ledit fichier dans la zone de protection du disque.

D'autres caractéristiques du procédé sont définies dans la suite de la description.

L'invention sera mieux comprise et d'autres caractéristiques et avantages apparaîtront à l'aide de la description ci-après et des dessins joints où :

- la Figure 1 est une représentation sous forme linéaire des tours de spirale d'un disque protégé ;
- la Figure 2 est un schéma du système selon l'invention entre éditeur et duplicateur pour la création d'un disque protégé ;
- la Figure 3 est un schéma de l'architecture logicielle de l'ensemble logiciel du système selon l'invention ; et
- la Figure 4 est un diagramme schématique de l'élément de protection chiffrement/déchiffrement.

Sur la Figure 1 est représentée une forme préférentielle de disque protégé, dans laquelle chaque spire (ou tour) d'une piste en spirale est représentée par un segment allant de l'extrémité gauche à l'extrémité droite de la figure. De même, on a indiqué l'intérieur du disque vers le bas de la figure, où commence une piste en spirale principale 1, et l'extérieur du disque où finit cette piste.

La piste principale 1 est une piste en spirale continue disposée sur toute la partie utile du disque et dont les secteurs ont, de manière classique, des adresses ordonnées sensiblement séquentiellement le long de cette piste. Une piste secondaire 2 est intercalée entre des spires successives de la piste principale, de manière que le pas de la piste reste, sensiblement dans toutes les zones du disque, constant et égal au pas standard habituellement utilisé dans les disques optiques classiques, tels que les disques CD- ou DVD-ROM. On appelle « zone de protection » ZDP la zone en deux parties où coexistent les deux pistes et où les mêmes adresses A à A + Q sont utilisées sur les deux parties ou pistes. On appellera « registre » l'association de deux secteurs ayant la même adresse respectivement sur la piste principale 1 et sur la piste secondaire 2. Comme on le verra, chaque secteur de la zone de protection comprend une information d'identification de la piste sur laquelle il se trouve. On désignera par pA la partie de la zone de protection appartenant à la piste principale et par pB la partie de la zone ZDP appartenant à la piste secondaire.

Il est clair qu'un lecteur standard effectuant des lectures successives d'une adresse donnée toujours dans les mêmes conditions a statistiquement toutes les chances de toujours lire le secteur de la même partie. La reconnaissance de la structure physique du disque, qui doit permettre de différencier un disque original à deux pistes d'une copie à une seule piste, consiste donc à effectuer une série de lectures d'un secteur de ZDP à partir d'une zone ZSA de la piste principale où les adresses sont inférieures à l'adresse recherchée (on a alors toutes les chances de lire le secteur sur la piste secondaire qui se présente en premier) suivie d'une série de lectures de la même adresse à partir d'une zone ZSR où les adresses sont supérieures à l'adresse recherchée (on a alors toutes les chances de lire le secteur sur la piste principale). Ainsi, si au bout de ces deux séries de lecture on a trouvé les deux informations d'identification différentes de la zone ZDP, on peut en conclure qu'on est bien en présence d'un disque original à deux pistes pA et pB.

Cependant, cette protection physique contre la copie peut ne pas être jugée suffisante et doit être complétée par une protection logicielle, qui met à profit ces particularités physiques afin de différencier un disque original d'une copie.

Les protections logicielles d'applications (jeux, encyclopédies,...) sont l'objet d'attaques de plusieurs types de pirates suivant qu'ils agissent pour des raisons ludiques (comprendre et « casser » un logiciel grâce à leurs compétences puis publier), économiques (contrefaçon et pressage de disques dé-protégés) ou anarchiques (diffuser le plus largement possible le patch d'une application, sans explication sur la méthode).

L'attaque la plus dangereuse pour un système de protection contre la copie est la création d'un patch et sa diffusion. Or, il est clair qu'empêcher la création d'un patch pour une application donnée est impossible ; mais on peut rendre cette tâche fastidieuse et difficile. Si, en outre, la protection est modifiée pour chaque application, obligeant à répéter la tâche en question, il n'est plus possible d'automatiser la génération du patch, permettant de contourner la protection, et le pressage de disques dé-protégés.

L'invention a donc pour objectifs d'empêcher la production d'un patch générique en rendant le système évolutif et de compliquer dans une large mesure l'analyse et la compréhension de la protection.

Pour cela, le système selon l'invention est basé sur le double principe de laisser à l'éditeur d'une application le soin de définir sa politique de protection et d'introduire des aléas dans la construction de l'ensemble de protection.

Le système de protection selon l'invention intervient à la fois chez l'éditeur d'une application à protéger et chez le duplicateur, ou presseur de disque, qui participent à l'écriture des données après transformation. La Figure 2 est un schéma global du système de protection et de sa mise en œuvre pour la création d'un disque optique protégé.

L'éditeur part de son application fonctionnelle 12 et décide des données sensibles qu'il souhaite dissimuler, du niveau de protection à adopter, des types de sanction à appliquer en cas de réalisation de copies pirates ou de tentatives d'intrusion, et des scénarios de dissuasion/diversion/leurrage destinés à perdre dans sa recherche et à décourager le pirate. Il met en œuvre cette stratégie de protection en utilisant sur sa station de travail une série d'outils logiciels fournis par un ensemble logiciel de création 10 qui permettent d'insérer les protections dans son application, de générer automatiquement les algorithmes et clefs de

protection des données en fonction du niveau de sécurité qu'il a choisi, de dissimuler des données choisies dans la zone de protection et d'implanter et positionner des leurres.

L'introduction des choix stratégiques effectués par l'éditeur est schématisée par l'entrée 15. Le système crée alors un fichier de protection mettant en œuvre ces choix qui est la représentation de la zone protégée. L'éditeur crée sur sa station de travail l'arborescence de son application, en disposant sans restriction de ses fichiers, et dispose dans cette arborescence (à l'endroit et sous le nom qu'il spécifie) le fichier de protection. L'application avec les protections ainsi implantées et positionnées est transférée sur un support de transport ou de transfert CD-R1 qui est de préférence un disque optique enregistrable. Ce support est adressé au duplicateur/presseur qui effectue alors sur sa station de travail 21 les opérations de pré-matriçage qui consistent à transformer, à partir d'un ensemble logiciel de pré-matriçage 20, les données du support CD-R1 sous la forme nécessaire pour procéder au matriçage et au pressage du disque protégé final. Ces données peuvent par exemple être enregistrées sur deux disques optiques enregistrables CD-R2 et CD-R3 qui contiennent respectivement les données à écrire sur la piste principale du disque final et sur la piste secondaire. Elles peuvent aussi être transférées par tout autre moyen de stockage et/ou de transfert d'informations protégé ou non (Ex : liaison de données, télécommunication avec ou sans cryptage, etc...).

L'ensemble logiciel de création du système selon l'invention est décrit par la définition d'un certain nombre d'éléments de protection et par l'enchaînement de ces éléments. L'ensemble logiciel intervient aussi bien lors de la création chez l'éditeur, où il génère un fichier de protection qui est la représentation du contenu de la zone de protection ZDP du disque final protégé, que lors du pré-matriçage chez le presseur et que lors de l'usage de l'application protégée par un utilisateur client de l'éditeur.

L'ensemble logiciel comprend un certain nombre de composants selon une architecture représentée sur la Figure 3 applicable à toute application cliente du système.

Ces composants incluent une interface 100 avec l'application cliente, un composant 103 d'accès au média 13 par secteur ainsi qu'à la zone de protection à deux parties, un composant 102 de gestion de la

procédure d'identification de piste et de formatage des données et une bibliothèque 101 contenant tous les algorithmes non protégés (calcul de codes vérificateurs du type CRC/Cyclic Redundancy code ou code de redondance cyclique, matriçages de données, algorithmes de chiffrement...). Ces composants sont copiés dans l'arborescence de l'application par l'éditeur à l'endroit et sous le nom que celui-ci choisit.

Parmi les éléments de protection disponibles dans l'ensemble logiciel de création du système selon l'invention, un premier d'entre eux est constitué par le positionnement variable de l'information d'identification de partie/piste dans la zone de protection. Cet élément de protection inclut une fonction de calcul de la position de l'information d'identification au sein de chaque secteur considéré en fonction de la position relative du secteur dans la zone de protection ZDP et de la position absolue du début de cette zone. On peut par exemple imaginer diverses lois de transformation pour passer de la valeur de la position absolue du secteur à une valeur comprise entre 0 et le nombre N d'octets du secteur, qui constituera la position de l'information d'identification ou de l'octet la contenant au sein du secteur.

Un avantage notable de ce positionnement variable est que la position de l'information d'identification change dès que la position de début de la zone de protection change, ce qui doit être le cas lorsque l'on change le contenu du disque (l'éditeur change ses choix).

Un autre élément de protection consiste en la dissimulation de données choisies par l'éditeur, notamment de données jugées sensibles par celui-ci. En effet, le but est de compliquer la récupération de données en dehors de l'application. Pour cela, le système permet d'implanter des données en les répartissant sur les pistes pA et pB de la zone de protection après les avoir transformées. Par exemple, pour chaque registre de la zone de protection, on tire un aléa k pour réaliser un matriçage des données reçues : les données initiales sont considérées comme un ensemble de matrices de taille k plus un reliquat éventuel et on permute dans chaque matrice les lignes avec les colonnes en conservant tel que le reliquat éventuel. Les données finales sont ensuite écrites pour moitié sur pA, pour moitié sur pB en y adjoignant l'information d'identification de piste adéquate et dans la position souhaitée.

L'ensemble logiciel de création peut proposer aussi comme élément de protection l'implantation de leurres. Le but d'un leurre est de faire croire que le fonctionnement de l'application est normal le plus longtemps possible, de manière à rendre très difficile la recherche de l'origine des effets anormaux que le leurre induira. L'implantation d'un leurre se fait dans les deux secteurs d'un registre de manière que la lecture d'une seule partie/piste de la zone de protection induise un fonctionnement apparemment correct mais différent de l'application, au moins pendant un certain temps, et moins bon le cas échéant.

Un autre élément de protection tendant à rendre complexe la récupération des données dans la zone de protection consiste en un chiffrement/déchiffrement de données selon un niveau de sécurité choisi par l'éditeur. Plusieurs niveaux de sécurité sont en effet disponibles et c'est l'éditeur qui doit choisir le bon compromis entre sécurité et rapidité puisqu'un algorithme est d'autant plus lent qu'il est plus sûr en règle générale. De préférence, le premier niveau consiste en un simple brouillage. Pour d'autres niveaux de sécurité, l'ensemble logiciel de création dispose de plusieurs algorithmes avec des temps d'exécution comparables et réalise lui-même, dans le niveau sélectionné, le choix d'un algorithme de manière aléatoire. Les clefs de chiffrement associées sont créées par le système et gérées par l'application. Pour protéger ces clefs applicatives, le système crée une clef de chiffrement privée qu'il gère lui-même. Un module de chiffrement contient le niveau de sécurité choisi, l'algorithme de chiffrement/déchiffrement (ou plus précisément son identifiant) et une clef privée. La clef applicative est connue de l'application seule qui la charge/décharge du module lors des opérations de chiffrement/déchiffrement.

Ceci est schématisé sur la Figure 4 où l'on reconnaît un module 30 avec la clef privée 31 et l'algorithme associé 32, la clef applicative 42 qui, associée en 33 à la clef privée, génère la clef volatile 34 nécessaire à l'algorithme 30 pour les opérations de chiffrement/déchiffrement 35 permettant de passer des données sources 40 de l'application aux données chiffrées 41 et vice-versa.

Un autre élément de protection important est constitué par une série de mesures anti-intrusion. Ces mesures ont pour objet d'empêcher l'analyse et la compréhension du fonctionnement de l'application

essentiellement par l'utilisation de débogueurs (exemple : SoftICE, marque déposée) et de contrôler que l'application ou ses données n'ont pas été modifiées.

Une première mesure consiste à interdire, dès le lancement de l'application, l'utilisation de débogueurs connus tel SoftICE. Ces mesures incluent par ailleurs une fonction de détection à la demande (de l'application) de la présence d'un débogueur. Le principe est de multiplier les vérifications en différents endroits pour compliquer le contournement.

On prévoit également une fonction de vérification de l'intégrité des codes à l'aide du calcul de CRCs. On peut notamment calculer les CRC 16 des divers composants du système d'origine puis vérifier ces codes lors du chargement de ces composants. Une fonction de vérification de signature du disque sur des données stockées dans la zone de protection peut également être prévue. Elle consiste par exemple à calculer le CRC 32 des données utiles d'un secteur lors de la création d'un disque et à vérifier cette valeur lors de l'utilisation.

Est également prévue une fonction de détection de temps d'exécution incorrect pour des fonctions prédéterminées.

Ces mesures anti-intrusion débouchent sur des contre-mesures déclenchées lorsqu'au moins une anomalie est détectée. Ces contre-mesures comprennent la mise du système en divers états selon la nature et la gravité de l'anomalie détectée. L'état instable se traduit par le fait qu'une lecture demandée d'un secteur provoque la lecture d'un autre secteur (données incorrectes), ou la lecture échoue parce qu'on est sorti de la zone de protection, ou la lecture ne se fait pas et des données incohérentes sont retournées à la place. Cet état instable peut être déclenché, sans avertissement à l'application, par la détection de la présence d'un débogueur lors de l'initialisation ou à la suite de l'utilisation de la fonction de vérification de signature.

L'état critique se traduit par l'arrêt sans préavis du système lors de toute action ultérieure entraînant une lecture dans la zone de protection. Cet état critique peut être déclenché par une initialisation s'effectuant mal ou par la détection de la présence d'un débogueur par la fonction de détection à la demande.

L'état bloqué se traduit par le blocage immédiat du système sans information ni préavis. Il est déclenché lorsque l'intégrité des codes n'est pas respectée ou en cas de temps d'exécution incohérent.

Ces éléments de protection ne mettent pas à l'abri d'une faille de sécurité chez l'éditeur. Aussi, il est prévu que le système soit auto-protégé et l'ensemble logiciel de création est donc fourni à l'éditeur sur un disque optique protégé lui-même par le système selon l'invention.

Lorsque le fichier de protection a été créé par l'éditeur et implanté dans l'arborescence de l'application qui est transcrite sur le disque de transport CD-R1, il est alors nécessaire de réaliser les opérations de pré-matriçage pour réécrire les données pour les disques CD-R2 et CD-R3 telles qu'elles seront présentes respectivement sur la piste principale et les pistes secondaires du disque final protégé. C'est le rôle de l'ensemble logiciel de pré-matriçage que de générer des images de données de ces disques. Cet ensemble comprend en particulier une fonction de calcul de début de la zone de protection à deux parties, une fonction de calcul de la position de l'information d'identification de piste et une fonction d'écriture de secteur pour placer ladite information d'identification à la position calculée pour ledit secteur.

Il est à noter que l'ensemble logiciel de création intervient dans l'ensemble logiciel de pré-matriçage, l'une des opérations de pré-matriçage étant de remplacer l'ensemble logiciel de création par un ensemble logiciel d'utilisation qui comprend des composants similaires renommés permettant l'accès aux fonctions de l'ensemble de création nécessaires dans le mode utilisation, mode qui permet à l'application protégée d'utiliser la protection.

La fonction de calcul du début de la zone de protection consiste à rechercher dans les secteurs lus dans les données du disque de transport CD-R1 un secteur de la piste principale pA contenant une information de début de zone de protection pour la piste pA suivi immédiatement d'un secteur de la piste pB contenant l'information de début de zone pour cette seconde partie et à vérifier que ces conditions ne se produisent qu'une seule fois et que le début de zone de protection est situé à des distances du début et de la fin de piste principale supérieures à des valeurs prédéterminées.

Quant à la fonction de calcul de la position de l'information d'identification de partie/piste, elle est de même type que celle décrite plus haut pour l'ensemble logiciel de création.

La solution préférée pour porter les données obtenues après le pré-matriçage est constituée par des disques optiques enregistrables classiques CD-R2 et CD-R3.

Bien entendu, les ensembles et fonctions précédemment décrits sont complétés par des fonctions classiques d'initialisation, d'écriture et de lecture de données ou de chargement/déchargement de fichier.

Il est clair que l'invention s'applique de façon préférentielle à un disque optique protégé du type à double piste physiquement distinctes. Mais la solution avec zone de protection à deux parties sur la même piste n'est pas exclue, moyennant les adaptations nécessaires.

Il est clair aussi que la description ci-dessus permet en même temps de définir un procédé de protection contre la copie d'informations correspondant utilisant ces mêmes principes de protection.

Bien entendu, les principes du système et du procédé selon l'invention resteront valables, même si d'autres éléments de protection peuvent être imaginés et ajoutés.

REVENDICATIONS

1. Système de protection contre la copie d'informations pour la création d'un disque optique protégé du type comportant au moins une piste principale en spirale, sur laquelle sont inscrites des marques d'information rangées dans des secteurs dont les adresses sont sensiblement séquentielles le long de la piste, et une zone de protection (ZDP) à deux parties sensiblement de même taille incluant chacune une série de secteurs désignés par des adresses identiques pour chaque partie, chaque secteur de la zone de protection incluant une information d'identification caractéristique de la partie à laquelle il appartient et l'une des parties au moins appartenant à ladite piste principale, ledit système étant caractérisé en ce qu'il comprend :

- un ensemble logiciel de création de protection (10) pour permettre la création, chez l'éditeur d'une application (12) destinée à être portée par ledit disque, d'un fichier de protection à partir d'éléments de protection dudit ensemble logiciel sélectionnés par l'éditeur et de données et paramètres choisis par l'éditeur ;
- un moyen de transport (CD-R1) comportant ladite application et ledit fichier de protection ainsi que la localisation des fichiers correspondants sur le disque protégé, selon une arborescence déterminée par l'éditeur ;
- un ensemble logiciel de pré-matriçage (20) pour, chez le duplicateur de disques et à partir des informations contenues dans ledit moyen de transport, déterminer et générer le contenu des deux parties dudit disque protégé ; et
- des moyens de stockage (CD-R2, CD-R3) respectivement des informations de la piste principale, avec la première partie de la zone de protection, et de la seconde partie de cette zone pour la réalisation par le duplicateur des opérations ultérieures de matriçage et duplication du disque protégé.

2. Système selon la revendication 1, caractérisé en ce que ledit ensemble logiciel de création comprend un élément de protection par positionnement variable de l'information d'identification de partie incluant une fonction de calcul de la position de l'information d'identification à l'intérieur du secteur considéré en fonction de la position relative du secteur dans la zone de protection et de la position absolue du début de ladite zone.

3. Système selon l'une des revendications 1 ou 2, caractérisé en ce que ledit ensemble logiciel de création comprend un élément de protection par dissimulation de données choisies par l'éditeur incluant une fonction de matriçage des données reçues pour chaque registre, constitué par deux secteurs associés de la zone de protection, à partir d'une valeur aléatoire k et d'écriture des données finales répartie entre les deux parties de ladite zone de protection.

4. Système selon la revendication 3, caractérisé en ce que ledit matriçage consiste, en considérant les données reçues comme un ensemble de matrices de taille k plus un reliquat éventuel, à permuter les lignes avec les colonnes desdites matrices en conservant le reliquat éventuel tel que.

5. Système selon l'une quelconque des revendications 1 à 4, caractérisé en ce que ledit ensemble logiciel de création comprend un élément de protection par implantation de leurres dans les deux secteurs associés d'un registre de la zone de protection de manière que la lecture d'une seule partie de la zone de protection induise un fonctionnement apparemment correct mais différent de l'application.

6. Système selon l'une quelconque des revendications 1 à 5, caractérisé en ce que ledit ensemble logiciel de création comprend un élément de protection par chiffrement/déchiffrement de données selon un niveau de sécurité choisi par l'éditeur.

7. Système selon la revendication 6, caractérisé en ce que ledit élément de protection par chiffrement/déchiffrement comprend :

- une collection d'algorithmes de chiffrement/déchiffrement affectés aux divers niveaux de sécurité, un algorithme du niveau choisi par l'éditeur étant sélectionné aléatoirement par le système lui-même ;
- une fonction de création d'une clef privée, ledit algorithme et sa clef privée étant stockés dans un module de chiffrement dans les deux secteurs associés d'un registre de la zone de protection ;
- une fonction de création de clef applicative par l'éditeur à partir des données dudit module de chiffrement, ladite clef applicative étant connue de l'application seule ;
- une fonction chiffrement/déchiffrement de données à partir dudit module et de ladite clef applicative.

8. Système selon l'une quelconque des revendications 1 à 7, caractérisé en ce que ledit ensemble logiciel de création comprend un élément de protection par mesures anti-intrusion incluant au moins l'une des mesures suivantes :

- une fonction de détection à la demande de présence de débogueur ;
- une fonction de vérification de l'intégrité des codes à partir du calcul de CRCs ;
- une fonction de vérification d'une signature du disque sur des données stockées dans ladite zone de protection ;
- une fonction de détection de temps d'exécution incorrect pour des fonctions déterminées dudit ensemble logiciel de création ;
- des contre-mesures déclenchées lorsque au moins une desdites fonctions des mesures anti-intrusion détecte une anomalie.

9. Système selon la revendication 8, caractérisé en ce que lesdites contre-mesures comprennent la mise du système soit en état instable où les données demandées ne sont pas lues ou sont modifiées sans avertissement, lorsque la présence d'un débogueur est détectée à l'initialisation du système ou lors de l'utilisation de la fonction de vérification

de signature, soit en état critique où toute action ultérieure entraînant une lecture dans la zone de protection provoque l'arrêt sans préavis du système, lorsque la présence d'un débogueur est détectée par ladite fonction de détection à la demande, soit en état bloquée où le système est bloqué sans information ni préavis, lorsque la fonction de vérification de l'intégrité des codes ou la fonction de détection de temps d'exécution détectent une anomalie.

10. Système selon l'une quelconque des revendications précédentes, caractérisé en ce que ledit fichier de protection inclut les composants (100 à 103) dudit ensemble logiciel de création.

11. Système selon l'une quelconque des revendications précédentes, caractérisé en ce que ledit ensemble logiciel de création (10) est porté par un disque optique lui-même protégé par le système selon l'une quelconque des revendications précédentes.

12. Système selon l'une quelconque des revendications précédentes, caractérisé en ce que ledit ensemble logiciel de pré-matriçage comprend des moyens pour générer une image des données à stocker dans lesdits moyens de stockage respectifs, lesdits moyens de génération d'images incluant une fonction de calcul de début de la zone de protection à deux parties, une fonction de calcul de la position de l'information d'identification de partie, identique à celle dudit ensemble logiciel de création, et une fonction d'écriture d'un secteur pour placer ladite information d'identification à la position calculée dans chaque secteur à inscrire dans lesdites images.

13. Système selon la revendication 12, caractérisé en ce que ladite fonction de calcul de début de la zone de protection consiste à rechercher dans les secteurs dudit moyen de transport (CD-R1) un secteur de ladite première partie contenant une information de début de zone de protection pour ladite partie, suivi d'un secteur de ladite seconde partie contenant l'information de début de zone de protection pour ladite seconde partie, et à vérifier que ces conditions ne sont réunies qu'une seule fois et

que le début de zone de protection trouvé est situé à des distances supérieures à des valeurs prédéterminées du début et de la fin de la piste principale.

14. Système selon l'une quelconque des revendications précédentes, caractérisé en ce que ledit moyen de transport (CD-R1) et lesdits moyens de stockage (CD-R2, CD-R3) sont des disques optiques enregistrables.

15. Procédé de protection contre la copie d'informations enregistrées sur un disque optique protégé du type comportant au moins une piste principale en spirale, sur laquelle sont inscrites des marques d'information rangées dans des secteurs dont les adresses sont sensiblement séquentielles le long de la piste, et une zone de protection (ZDP) à deux parties sensiblement de même taille incluant chacune une série de secteurs désignés par des adresses identiques pour chaque partie, chaque secteur de la zone de protection incluant une information d'identification caractéristique de la partie à laquelle il appartient et l'une des parties au moins appartenant à ladite piste principale, ledit procédé étant caractérisé en ce qu'il consiste à créer un fichier de protection à partir d'éléments de protection logicielle sélectionnés lors de la création dudit fichier et à enregistrer ledit fichier dans la zone de protection du disque.

16. Procédé selon la revendication 15 , caractérisé en ce qu'un élément de protection est constitué par le positionnement variable de l'information d'identification de partie et en ce que ledit procédé inclut de manière correspondante une étape consistant à calculer la position de l'information d'identification à l'intérieur du secteur considéré, en fonction de la position relative du secteur dans la zone de protection et de la position absolue du début de ladite zone.

17. Procédé selon l'une des revendications 15 ou 16, caractérisé en ce qu'un élément de protection est constitué par la dissimulation de données choisies par un éditeur créant ledit fichier de protection et en ce que ledit procédé inclut de manière correspondante des étapes de :

- transformer les données choisies selon une loi de transformation donnée ; et
- implanter les données obtenues selon ladite loi de transformation de manière répartie entre les deux parties de ladite zone de protection.

18. Procédé selon la revendication 17, caractérisé en ce que ladite étape de transformer les données choisies comprend les étapes de :

- tirer un aléa k ;
- subdiviser, pour chaque registre, constitué par deux secteurs associés des deux parties de la zone de protection, les données selon des matrices de taille k plus un reliquat éventuel ;
- permuter dans chaque matrice les lignes avec les colonnes en conservant le reliquat éventuel tel quel.

19. Procédé selon l'une quelconque des revendications 15 à 18, caractérisé en ce qu'un élément de protection est constitué par l'implantation de leurres dans les deux secteurs associés d'un registre de la zone de protection de manière que la lecture d'une seule partie de la zone de protection induise un fonctionnement apparemment correct mais différent de l'application enregistrée sur le disque protégé.

20. Procédé selon l'une quelconque des revendications 15 à 19, caractérisé en ce qu'un élément de protection est constitué par le chiffrement/déchiffrement de données selon un niveau de sécurité choisi par un éditeur d'une application créant ledit fichier de protection pour cette application et en ce que ledit procédé inclut de manière correspondante les étapes de :

- choisir un niveau de sécurité pour ledit chiffrement/déchiffrement ;
- choisir aléatoirement, dans le niveau de sécurité sélectionné, un algorithme de chiffrement/déchiffrement ;
- créer une clef privée associée audit algorithme ;

- stocker ledit algorithme et ladite clef privée dans un module de chiffrement contenu dans les deux secteurs associés d'un registre de ladite zone de protection ;
- créer, sous le contrôle de l'éditeur, une clef applicative à partir des données dudit module ;
- chiffrer/déchiffrer les données à partir des éléments dudit module et de ladite clef applicative associée.

21. Procédé selon l'une quelconque des revendications 15 à 20, caractérisé en ce qu'un élément de protection est constitué par des mesures anti-intrusion et en ce que ledit procédé inclut de manière correspondante au moins une des étapes suivantes :

- détecter à la demande la présence d'un débogueur ;
- vérifier l'intégrité de codes dudit fichier de protection par calcul de CRCs ;
- vérifier une signature du disque sur des données stockées dans ladite zone de protection ;
- vérifier le temps d'exécution d'étapes prédéterminées dudit procédé ;
- déclencher des contre-mesures lorsqu'au moins une desdites étapes conduit à la détection d'une anomalie.

22. Procédé selon la revendication 21, caractérisé en ce que ladite étape de vérifier l'intégrité de codes comprend :

- le calcul de CRCs de composants logiciels lors de la création dudit fichier de protection ;
- la vérification desdits CRCs lors du chargement desdits composants.

23. Procédé selon l'une des revendications 21 ou 22, caractérisé en ce que ladite étape de vérifier une signature comprend :

- le calcul d'un CRC des données utiles d'un secteur lors de la création dudit fichier de protection ;
- la vérification de la valeur dudit CRC lors de l'utilisation dudit secteur.

24. Procédé selon l'une quelconque des revendications 21 à 23, caractérisé en ce que lesdites contre-mesures comprennent au moins une des mesures suivantes :

- mise en état instable du système utilisateur dudit disque lorsque la présence d'un débogueur est détectée lors de l'initialisation ou lors de ladite étape de vérification de signature ;
- mise en état critique dudit système utilisateur dudit disque lorsque la présence d'un débogueur est détectée lors de ladite étape de détection à la demande ;
- mise en état bloqué dudit système utilisateur dudit disque lorsqu'une anomalie est détectée lors desdites étapes de vérification de l'intégrité de codes et/ou de vérification du temps d'exécution.

25. Procédé selon la revendication 24, caractérisé en ce que la mise en état instable consiste en ce que les données demandées par le système ne sont pas lues ou sont modifiées sans avertissement.

26. Procédé selon l'une des revendications 24 ou 25, caractérisé en ce que la mise en état critique consiste en ce que toute lecture ultérieure dans la zone de protection provoque l'arrêt sans préavis du système.

27. Procédé selon l'une quelconque des revendications 24 à 26, caractérisé en ce que la mise en état bloqué consiste en un blocage sans information ni préavis du système.

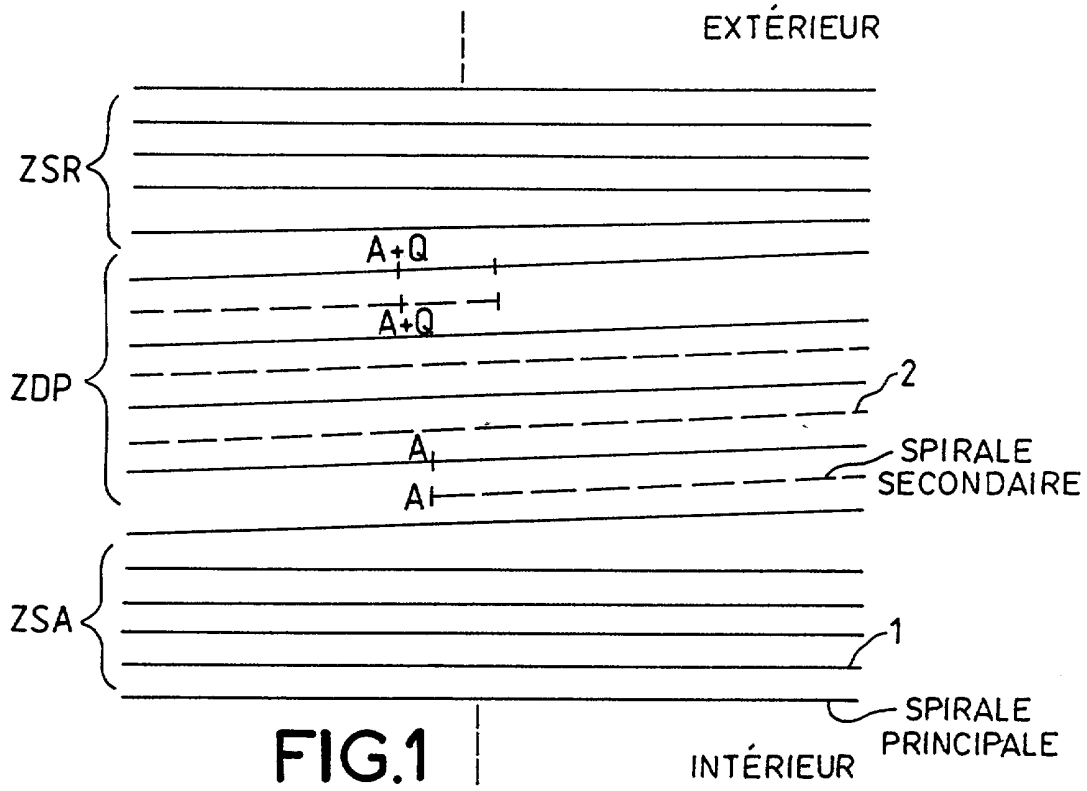

EXTÉRIEUR
ZSR
ZDP
ZSA
A+Q
A+Q
A
A
2
SPIRALE SECONDAIRE
1
SPIRALE PRINCIPALE
INTÉRIEUR

FIG.1

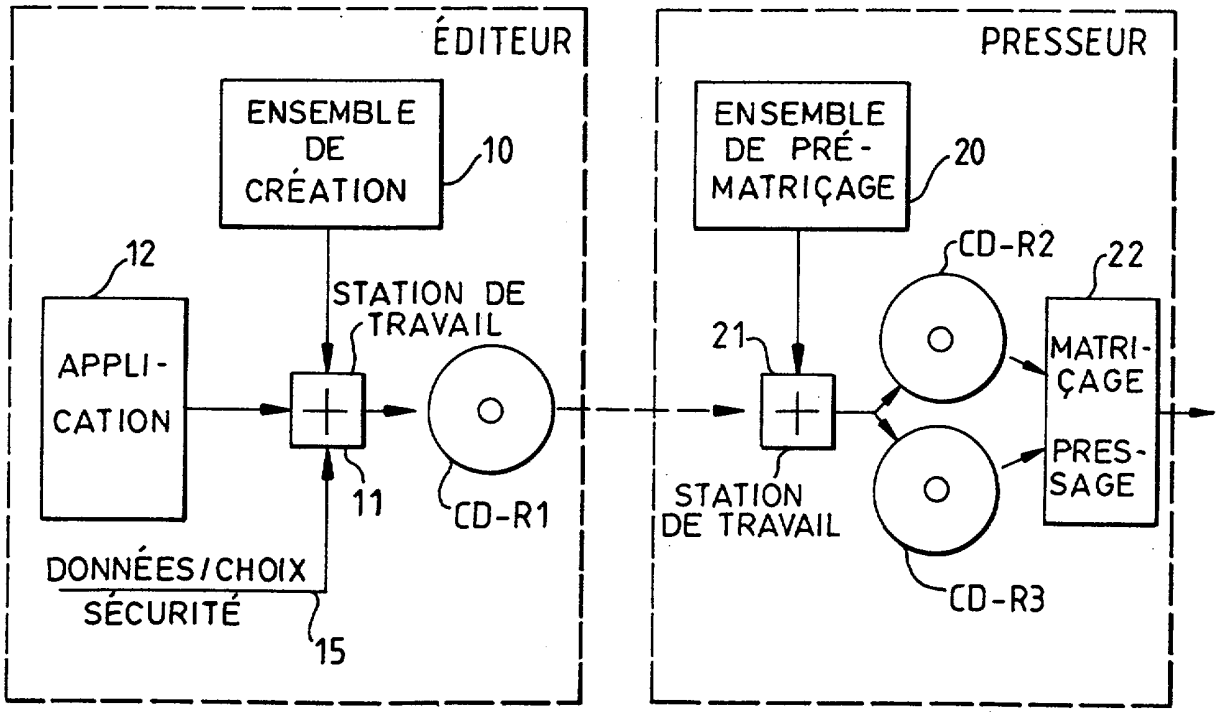

ÉDITEUR
ENSEMBLE DE CRÉATION
10
12
APPLI-CATION
STATION DE TRAVAIL
11
CD-R1
DONNÉES/CHOIX SÉCURITÉ
15
PRESSEUR
ENSEMBLE DE PRÉ-MATRIÇAGE
20
21
CD-R2
22
MATRI-ÇAGE
PRES-SAGE
STATION DE TRAVAIL
CD-R3

FIG.2

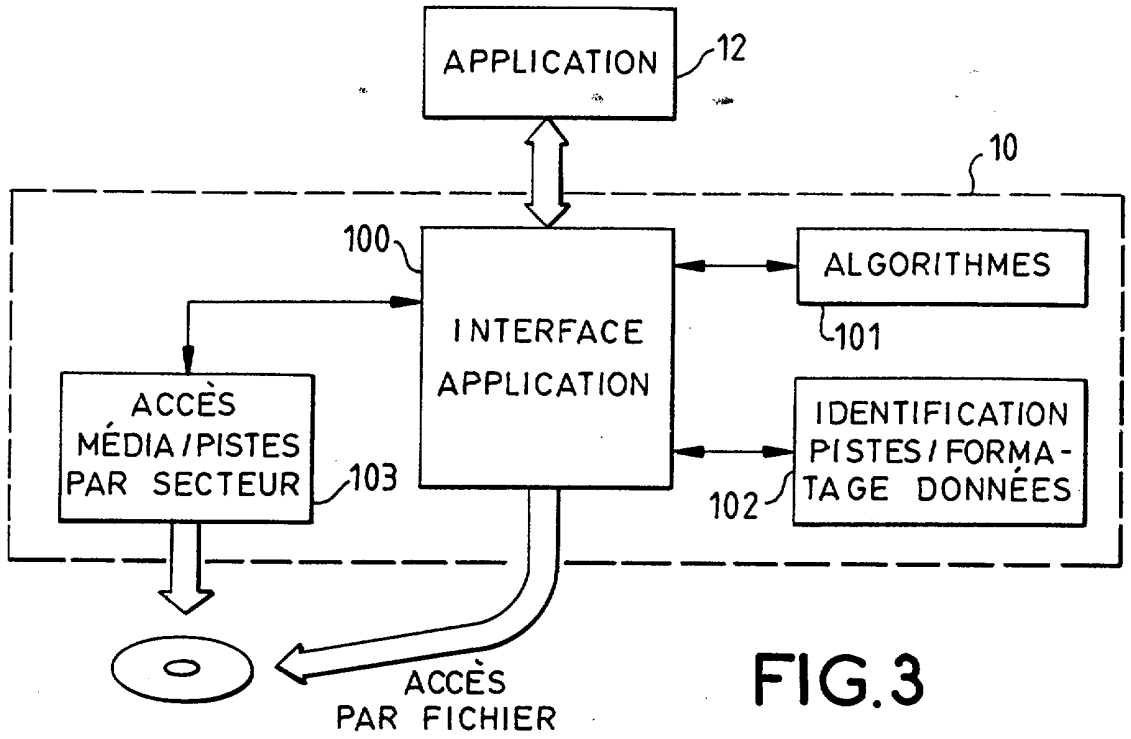

APPLICATION
12
10
100
INTERFACE APPLICATION
ALGORITHMES
101
ACCÈS MÉDIA/PISTES PAR SECTEUR
103
IDENTIFICATION PISTES/FORMATAGE DONNÉES
102
ACCÈS PAR FICHIER

FIG.3

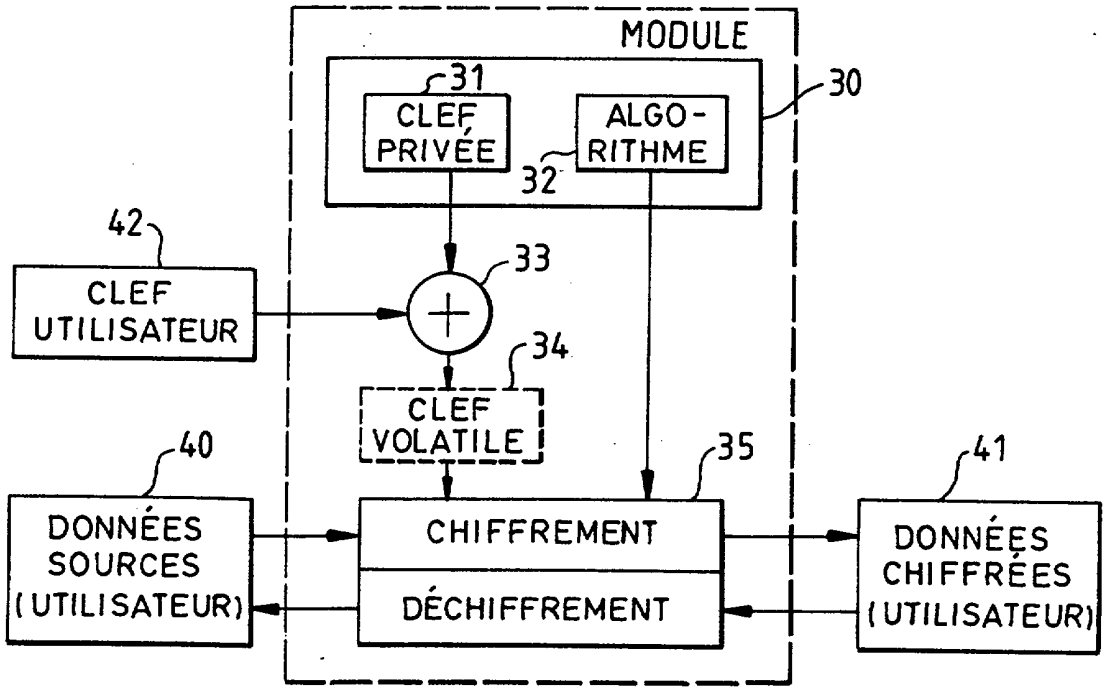

MODULE
31
CLEF PRIVÉE
ALGORITHME
32
30
42
CLEF UTILISATEUR
33
34
CLEF VOLATILE
40
35
41
DONNÉES SOURCES (UTILISATEUR)
CHIFFREMENT
DÉCHIFFREMENT
DONNÉES CHIFFRÉES (UTILISATEUR)

FIG.4

RÉPUBLIQUE FRANÇAISE

INPI
INSTITUT NATIONAL DE LA PROPRIETE INDUSTRIELLE

2820843

N° d'enregistrement national

FA 598488
FR 0101808

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		
Y	US 5 761 301 A (GOTOH YOSHIHO ET AL) 2 juin 1998 (1998-06-02)	1,15	G06F9/44 G06K19/06
A	* colonne 7, ligne 8 - ligne 35; figures 1,36,37 *	6,20	G11B7/00
Y	FR 2 787 232 A (THOMSON CSF) 16 juin 2000 (2000-06-16) * le document en entier *	1,15	
A	FR 2 769 119 A (THOMSON CSF) 2 avril 1999 (1999-04-02) * le document en entier *	1,15	
A	US 5 752 009 A (NAKAHARA MASARU ET AL) 12 mai 1998 (1998-05-12) * colonne 15, ligne 18 - ligne 21; figures 8,15 *	1,6,15, 20	
A	US 6 028 936 A (HILLIS W DANIEL) 22 février 2000 (2000-02-22) * colonne 8, ligne 22 - colonne 12, ligne 16 * * colonne 4, ligne 47 - ligne 67 *	1,6,8, 15,20,21	DOMAINES TECHNIQUES RECHERCHÉS (Int.CL.7) G11B G06F
A	DE 196 02 804 A (HARRAS ROLAND) 31 juillet 1997 (1997-07-31) * revendication 14 *	8,21	

Date d'achèvement de la recherche	Examinateur
14 décembre 2001	Brunet, L

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)

ANNEXE AU RAPPORT DE RECHERCHE PRÉLIMINAIRE RELATIF A LA DEMANDE DE BREVET FRANÇAIS NO. FR 0101808 FA 598488

La présente annexe indique les membres de la famille de brevets relatifs aux documents brevets cités dans le rapport de recherche préliminaire visé ci-dessus.
Les dits membres sont contenus au fichier informatique de l'Office européen des brevets à la date du 14-12-2001
Les renseignements fournis sont donnés à titre indicatif et n'engagent pas la responsabilité de l'Office européen des brevets, ni de l'Administration française

Document brevet cité au rapport de recherche	Date de publication	Membre(s) de la famille de brevet(s)	Date de publication
US 5761301 A	02-06-1998	CN 1127049 A	17-07-1996
		CN 1138915 A	25-12-1996
		DE 69523139 D1	15-11-2001
		EP 1120777 A2	01-08-2001
		EP 0706174 A1	10-04-1996
		EP 0741382 A1	06-11-1996
		JP 8273164 A	18-10-1996
		WO 9528704 A1	26-10-1995
		WO 9616401 A1	30-05-1996
		US 5881038 A	09-03-1999
		US 5805551 A	08-09-1998
		CN 1166223 A	26-11-1997
		CN 1173942 A	18-02-1998
		DE 69610859 D1	07-12-2000
		DE 69610859 T2	15-03-2001
		DE 69610860 D1	07-12-2000
		DE 69610860 T2	15-03-2001
		DE 69610861 D1	07-12-2000
		DE 69610861 T2	15-03-2001
		DE 69611906 D1	05-04-2001
		DE 69611906 T2	21-06-2001
		DE 69613010 D1	28-06-2001
		DE 69613010 T2	15-11-2001
		DE 69613011 D1	28-06-2001
		DE 69613011 T2	15-11-2001
		DE 69613156 D1	05-07-2001
		DE 69613156 T2	25-10-2001
		DE 69614580 D1	20-09-2001
		DE 69614823 D1	04-10-2001
		DE 69615418 D1	25-10-2001
		EP 1005033 A1	31-05-2000
		EP 1005034 A1	31-05-2000
		EP 1005023 A1	31-05-2000
		EP 1005024 A1	31-05-2000
		EP 1005025 A1	31-05-2000
		EP 1005026 A1	31-05-2000
		EP 1005027 A1	31-05-2000
		EP 1024478 A1	02-08-2000
		EP 1005028 A1	31-05-2000
		EP 1003162 A1	24-05-2000
		EP 1005035 A1	31-05-2000
		EP 1006516 A1	07-06-2000
		EP 1006517 A1	07-06-2000
		EP 1028422 A1	16-08-2000
		EP 1028423 A1	16-08-2000
		EP 1030297 A1	23-08-2000

EPO FORM P0465

Pour tout renseignement concernant cette annexe : voir Journal Officiel de l'Office européen des brevets, No.12/82

ANNEXE AU RAPPORT DE RECHERCHE PRÉLIMINAIRE RELATIF A LA DEMANDE DE BREVET FRANÇAIS NO. FR 0101808 FA 598488

La présente annexe indique les membres de la famille de brevets relatifs aux documents brevets cités dans le rapport de recherche préliminaire visé ci-dessus.
Les dits membres sont contenus au fichier informatique de l'Office européen des brevets à la date du 14-12-2001
Les renseignements fournis sont donnés à titre indicatif et n'engagent pas la responsabilité de l'Office européen des brevets, ni de l'Administration française

Document brevet cité au rapport de recherche		Date de publication	Membre(s) de la famille de brevet(s)		Date de publication
US 5761301	A		EP	1031974 A1	30-08-2000
			EP	0807929 A1	19-11-1997
			EP	0802527 A1	22-10-1997
FR 2787232	A	16-06-2000	FR	2787232 A1	16-06-2000
			AU	1569400 A	03-07-2000
			EP	1159742 A1	05-12-2001
			WO	0036601 A1	22-06-2000
FR 2769119	A	02-04-1999	FR	2769119 A1	02-04-1999
			AU	9270198 A	23-04-1999
			BR	9815393 A	16-01-2001
			CN	1271452 T	25-10-2000
			EP	1018113 A1	12-07-2000
			WO	9917281 A1	08-04-1999
			JP	2001518674 T	16-10-2001
US 5752009	A	12-05-1998	EP	1076331 A2	14-02-2001
			EP	0634741 A1	18-01-1995
			JP	2891877 B2	17-05-1999
			JP	7078187 A	20-03-1995
			KR	186891 B1	15-04-1999
US 6028936	A	22-02-2000	AUCUN		
DE 19602804	A	31-07-1997	DE	19602804 A1	31-07-1997

EPO FORM P0465

Pour tout renseignement concernant cette annexe : voir Journal Officiel de l'Office européen des brevets, No.12/82