(19) RÉPUBLIQUE FRANÇAISE

INSTITUT NATIONAL
DE LA PROPRIÉTÉ INDUSTRIELLE

PARIS

(11) N° de publication : 2 535 885
(à n'utiliser que pour les commandes de reproduction)

(21) N° d'enregistrement national : 83 12643

(51) Int Cl³ : G 11 B 15/04, 5/02.

(12) DEMANDE DE BREVET D'INVENTION A1

(22) Date de dépôt : 1er août 1983.

(30) Priorité US, 8 novembre 1982, n° 439,807.

(43) Date de la mise à disposition du public de la demande : BOPI « Brevets » n° 19 du 11 mai 1984.

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

(71) Demandeur(s) : *Société dite : VAULT CORPORATION.* — US.

(72) Inventeur(s) : William Krag Brotby.

(73) Titulaire(s) :

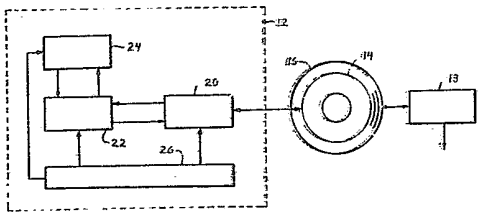
(74) Mandataire(s) : Lavoix.

(54) Procédé et appareil pour déjouer le copiage non autorisé de données enregistrées.

(57) L'invention concerne la protection d'un support d'enregistrement contre la réalisation de copies non autorisées.

Une procédure de contrôle de sécurité est incorporée dans le sous-programme d'initialisation qui est enregistré sur un disque 16 constituant une copie autorisée, et qui est exécuté avant la lecture des données protégées. La procédure de contrôle comprend un test qui détermine si le disque porte une marque caractéristique d'un disque autorisé. Cette marque peut être une signature magnétique qui est enregistrée sur une piste spécialisée 14 du disque et qui est modifiée par un appareil spécial 12 incorporé dans la pochette du disque, chaque fois que le disque est utilisé.

Application à la protection de logiciels commercialisés sous forme de disques souples.



FR 2 535 885 - A1

La présente invention concerne le domaine des mémoires d'ordinateur, et elle porte plus particulièrement sur la combinaison d'un procédé et d'un appareil qui déjoue le copiage non autorisé de données protégées qui ont été enregistrées sur un disque souple ou un autre support de mémoire.

Des milliards de francs sont dépensés chaque année pour l'achat de logiciels d'ordinateur. Le logiciel est vendu de façon caractéristique sous la forme d'un enregistrement sur un disque souple. Une fois que le client a chargé le programme dans la mémoire centrale de son ordinateur, à partir du disque souple, on peut concevoir qu'il lise le programme dans la mémoire et l'enregistre sur un second disque souple, créant ainsi une copie non autorisée du programme. On a estimé que 50% de l'ensemble des logiciels ont été copiés sans autorisation.

Le propriétaire du logiciel qui a été enregistré sur une copie autorisée et vendu à un client désire empêcher le client de réaliser et de vendre des copies non autorisées. L'invention permet de réaliser des copies, mais avec l'invention les copies sont inutilisables et donc sans valeur.

De façon caractéristique, les instructions et autres données enregistrées sur le disque en usine comprennent une procédure d'initialisation et un programme d'application principal. La procédure d'initialisation assure le formatage et d'autres procédures opérationnelles, parmi lesquelles l'établissement d'un répertoire du système d'exploitation qui indique à l'ordinateur l'emplacement réel, dans le matériel, auquel se trouveront certains fichiers.

Le brevet U S 4 214 280 décrit un procédé et un appareil pour enregistrer des données sur un disque comportant des zones défectueuses. Le procédé localise la zone défectueuse de façon à permettre d'écrire des

données sur les parties du disque qui ne sont pas défectueuses. L'invention décrite dans ce brevet vise non pas à protéger les données enregistrées contre la copie, mais à permettre l'utilisation de disques défectueux. Les défauts ne sont pas introduits intentionnellement et aucune tentative n'est faite pour écrire des données dans les zones défectueuses.

Un article de A. F. Shugart intitulé "Recorded Data Security Device", paru dans IBM Technical Disclosure Bulletin, Vol. 4, N° 10, mars 1962, décrit un dispositif qui empêche la lecture de certaines données protégées sur une mémoire à disques. La mémoire à disques consiste dans ce cas en au moins deux disques montés de façon à tourner sur un axe commun. L'un des disques contient des signaux de commande enregistrés qui commandent le fonctionnement des têtes de lecture/écriture des disques restants. Sous l'effet de signaux de sécurité enregistrés sur le premier disque, les têtes de lecture/écriture des disques restants sont déconnectées électriquement de leurs amplificateurs, ce qui empêche la lecture des données protégées. Bien que le dispositif décrit dans cet article utilise un canal spécial dans un but de sécurité, l'utilisation qui est faite de ce canal est totalement différente des techniques qui sont employées dans l'invention.

Le brevet U S 4 086 634 décrit un procédé et un appareil pour empêcher la copie non autorisée de bandes magnétiques. Le procédé consiste à enregistrer sur une bande magnétique un signal modulé de haute fréquence, en compagnie de l'information utile audible, de façon qu'une copie ultérieure de l'information utile et du signal modulé sur une bande magnétique, de façon non autorisée, avec un enregistrement classique utilisant une polarisation de haute fréquence, produise sur la bande copiée des signaux pa-

rasites identifiables produisant un bruit de reproduction audible qui gâche la bande copiée. Bien que l'invention du brevet précité vise à interdire la copie non autorisée d'une information enregistrée, son procédé est entièrement différent de la technique utilisée dans la présente invention.

L'invention est essentiellement destinée à l'utilisation avec des disques souples sur lesquels un logiciel a été enregistré et qui sont distribués en grandes quantités à des clients. Un but principal de l'invention est d'empêcher le client de réaliser une copie non autorisée de la copie autorisée qu'il a achetée.

Le client à évidemment le droit d'utiliser sa copie autorisée pour le but prévu et, pour cette raison, les inventions qui interdisent l'accès aux données enregistrées ne sont pas applicables au problème considéré. Au contraire, l'invention entre dans la catégorie des techniques destinées à empêcher une copie non autorisée de l'information protégée, c'est-à-dire la production d'un disque non autorisé. Simultanément, l'invention ne s'oppose pas au droit du client à lire l'information protégée.

Comme on le verra ci-après, l'invention ne peut pas empêcher le client de tenter de transcrire l'information protégée sur un disque non autorisé, mais elle fait effectivement en sorte que la copie non autorisée soit inutilisable.

La mise en oeuvre de l'invention exige une combinaison d'un appareil et d'un procédé.

Des disques autorisés fabriqués conformément à l'invention sont physiquement distinguables des disques vierges que des clients utiliseraient pour réaliser des copies non autorisées. Dans certains modes de réalisation de l'invention, les modifications qui carac-

térisent les disques autorisés sont relativement simples et ne peuvent pas être détectées aisément. On peut considérer que les caractéristiques physiques (marques) qui distinguent les disques autorisés constituent une empreinte digitale d'identification pour ces disques.

L'aspect "procédé" de l'invention est centré sur une procédure de contrôle de sécurité qui est incorporée dans le sous-programme d'initialisation qui est enregistré sur le disque autorisé et qui est exécutée avant la lecture de données protégées quelconques. Les données protégées peuvent être de façon caractéristique un programme d'application, mais dans d'autres circonstances, les données protégées peuvent comprendre des données de diverses formes, parmi lesquelles (de façon non limitative) des signaux binaires et des signaux analogiques.

Le sous-programme d'initialisation doit être exécuté avant que l'information protégée puisse être lue sur le disque, et le sous-programme d'initialisation commande la tête de lecture/écriture de l'ordinateur.

La procédure de contrôle de sécurité fait intervenir un test destiné à déterminer si le disque sur lequel elle a été enregistrée comporte ou non l'empreinte digitale physique qui est la marque caractéristique d'un disque autorisé. Si l'empreinte digitale est présente, la procédure de contrôle de sécurité autorise la tête de lecture/écriture à lire l'information protégée; cependant, si l'empreinte digitale est absente, comme ce serait le cas pour un disque non autorisé, la procédure de contrôle de sécurité empêche la tête de lecture/écriture de lire l'information protégée.

Dans un mode de réalisation préféré, si l'empreinte digitale est absente, la procédure de contrôle de sécurité ordonne à la tête de lecture/écriture d'effacer

l'information protégée.

Ainsi, l'information enregistrée sur un disque, comprenant le sous-programme d'initialisation ainsi que l'information protégée, peut être transcrite sur un disque non autorisé. L'information enregistrée sera identique sur le disque autorisé et sur le disque non autorisé.

Cependant, lorsqu'on tente d'utiliser le disque non autorisé, la procédure de contrôle de sécurité détermine que l'empreinte digitale distinctive qui caractérise un disque autorisé est absente, et à ce point, la procédure de contrôle de sécurité interdit la lecture de l'information protégée ou efface cette information.

L'invention sera mieux comprise à la lecture de la description qui va suivre de modes de réalisation, donnés à titre d'exemples non limitatifs. La suite de la description se réfère au dessin annexé qui est un schéma synoptique de l'appareil utilisé dans le troisième mode de réalisation de l'invention.

Premier mode de réalisation

Dans un premier mode de réalisation, qui est préféré pour sa simplicité, on crée intentionnellement en usine une zone défectueuse permanente localisée sur le disque non enregistré, à une position aléatoire sur la surface d'enregistrement, sur la partie de la surface d'enregistrement qui est réservée à l'information à protéger. Le défaut fait que la partie affectée du disque est incapable d'assurer une reproduction exacte d'un élément de données qu'une tête d'écriture a tenté précédemment d'enregistrer sur le défaut.

Ensuite, en usine, on détermine la position exacte du défaut sur le disque. Dans un mode de réalisation, on effectue ceci en enregistrant des 1 à toutes les positions, puis en relisant les données. Les positions dans lesquelles on ne relit pas des 1 constituent la zone défectueuse.

L'ordinateur considère comme un fichier (qu'on appellera Fichier D) l'ensemble des positions qui constituent le défaut, et la position de ce fichier est mémorisée dans la procédure d'initialisation qui est enregistrée sur le disque. La procédure d'initialisation comprend également des opérations qui constituent le contrôle de sécurité.

A ce point, on peut enregistrer sur le disque, en usine, le programme d'application principal ou d'autres données à protéger. Selon une variante, à ce point, on peut vendre le disque à quelqu'un qui désire enregistrer sur le disque un programme protégé.

Ensuite, chaque fois que le disque est lu, la procédure d'initialisation comprenant le contrôle de sécurité est exécutée. La procédure de contrôle de sécurité comprend les opérations consistant à ouvrir le Fichier D, à écrire un élément de données particulier dans ce fichier, à fermer le fichier, à rouvrir le Fichier D, à lire le contenu, et à comparer le contenu avec l'élément de données particulier qui a été écrit. Si les données lues sont identiques aux données écrites (comme ce serait le cas si le disque était une copie non autorisée ne contenant pas de défaut),la procédure de contrôle de sécurité ordonne d'ouvrir les fichiers dans lesquels les données protégées sont mémorisées, et d'effacer leur contenu.

Si les données lues diffèrent des données qui ont été écrites (comme il est normal pour un disque autorisé du fait qu'il contient un défaut), la procédure de contrôle de sécurité autorise la lecture des données protégées. Ainsi, une copie non autorisée du disque ne fournit pas les données protégées, ce qui rend vain un copiage non autorisé.

Second mode de réalisation

Dans un second mode de réalisation, qui procure

un niveau de sécurité supérieur à celui du premier mode de réalisation, on utilise un support d'enregistrement spécial sur une bande du disque. Cette bande peut comprendre plusieurs pistes.

Le support d'enregistrement spécial est une matière qui peut être enregistrée par une tête d'enregistrement spéciale dans l'usine dans laquelle le disque est fabriqué, mais qui ne peut pas être enregistrée avec la tête de lecture/écriture d'un ordinateur quelconque avec lequel le disque pourrait être utilisé.

Dans un mode de réalisation, le support d'enregistrement spécial est une matière ferromagnétique ayant des domaines si grands qu'ils ne peuvent être magnétisés que par l'application d'un champ magnétique supérieur à celui que produisent les têtes de lecture/écriture des ordinateurs existants.

Selon une autre forme, le support d'enregistrement spécial est une matière magnétique "plus dure" que la matière utilisée sur les disques souples ordinaires, ce qui fait que le champ magnétique limité que produisent les têtes d'écriture des ordinateurs existants ne peut pas écrire sur le support d'enregistrement spécial. De plus, le support d'enregistrement spécial doit avoir une coercivité grande par rapport au champ magnétique que produisent les têtes d'écriture/effacement d'ordinateurs existants, afin que l'ordinateur ne puisse pas effacer les données écrites dans le support d'enregistrement spécial.

Les pistes sur lesquelles le support d'enregistrement spécial est utilisé constituent ainsi une mémoire morte que la tête de lecture/écriture de l'ordinateur peut lire, mais dans laquelle elle ne peut pas écrire ou faire des changements.

Lorsque le disque est fabriqué en usine, la tête d'enregistrement spéciale écrit sur les pistes du

support d'enregistrement spécial un nombre (tel qu'une suite de "1") qui constitue une "empreinte digitale" permanente.

Une procédure d'initialisation du programme ordonne d'ouvrir le fichier qui se trouve dans les pistes spéciales et d'emplir ce fichier avec des 0.

Si maintenant le disque est un disque normal sur lequel le programme a été copié sans autorisation, cet ordre sera exécuté et le fichier qui se trouve à l'emplacement des pistes spéciales sera emplit avec des 0.

Cependant, si le disque lu est un disque autorisé (c'est-à-dire un disque qui comprend les pistes spéciales), la tête d'enregistrement de l'ordinateur sera incapable d'affecter les pistes spéciales, qui continueront à conserver le nombre constituant "l'empreinte digitale".

Le contrôle de sécurité demande ensuite la lecture du fichier. Si la lecture ne donne que des 0, le sous-programme de sécurité ordonne d'ouvrir tous les fichiers, y compris le programme d'application principal, et de les emplir de nombres dépourvus de signification, ce qui rend la copie inutile. Si le nombre lu est celui qui correspond à "l'empreinte digitale", le sous-programme de contrôle de sécurité autorise la lecture du programme d'application principale.

Troisième mode de réalisation

Un troisième mode de réalisation, représenté sur la figure unique, permet d'obtenir un niveau de sécurité plus élevé que ce qui est possible avec les premier et second modes de réalisation. Le troisième mode de réalisation nécessite cependant un appareil spécial, 12, qui fait partie intégrante de la pochette du disque.

Dans le troisième mode de réalisation, une piste 14 du disque 16 est spécialisée pour l'utilisation exclusive avec la procédure de contrôle de sécurité.

Lorsque le disque 16 quitte l'usine et avant qu'il ait été utilisé, cette piste spécialisée contient un signal de synchronisation suivi par un Fichier X qui contient un nombre déterminé N_o. Le même nombre N_o est contenu dans le programme de contrôle de sécurité, en langage machine, dans un Fichier Y.

Lorsque le disque 16 est introduit dans l'ordinateur, ce dernier exécute tout d'abord le sous-programme d'initialisation, avant que le programme d'application principal ou d'autres données à protéger ne soient chargés dans la mémoire centrale de l'ordinateur (à partir de laquelle ils pourraient être transcrits sur un autre disque, dans le but de réaliser une copie non autorisée). La procédure de contrôle de sécurité termine le sous-programme d'initialisation.

La procédure de contrôle de sécurité comprend des instructions qui incrémentent le nombre N_o contenu initialement dans le Fichier Y, pour donner un nouveau nombre N_1, qui est ensuite enregistré dans le fichier Y. Le nombre contenu dans le Fichier Y est ensuite comparé au nombre présent dans le Fichier X. Si les nombres sont égaux, l'ordinateur reçoit l'autorisation de lire et de charger en mémoire le programme d'application principal . Si les nombres ne sont pas égaux, l'ordinateur reçoit l'instruction d'effacer tous les fichiers, y compris ceux contenant le programme d'application principal.

On voit clairement qu'on obtient ce dernier résultat sauf si le nombre N_o enregistré initialement dans le Fichier X a été incrémenté précédemment de la même quantité que le nombre N_o enregistré initialement dans le Fichier Y.

Un appareil spécial 12 est incorporé dans la pochette du disque et fait partie intégrante de cette pochette. Cet appareil spécial a pour but d'incrémenter

le nombre présent dans le Fichier X, chaque fois que le disque 16 est lu. L'augmentation de ce nombre a lieu pendant les deux premiers tours du disque 16 et est donc terminée avant que la procédure de contrôle de sécurité ne soit exécutée. En utilisation normale, l'appareil spécial 12 fait en sorte que le nombre contenu dans le Fichier X soit égal au nombre contenu dans le Fichier Y, ce qui fait que le programme d'application principal peut être lu et chargé dans la mémoire centrale de l'ordinateur par la tête de lecture/écriture 18 de l'ordinateur, sous la commande du sous-programme d'initialisation.

Si une copie non autorisée des données protégées est effectuée une fois que les données ont été chargées dans la mémoire centrale de l'ordinateur, et si cette copie est enregistrée sur un disque classique, au lieu d'un disque de sécurité conforme à l'invention, la copie sera inutilisable, du simple fait que le disque classique ne comporte pas l'appareil spécial 12 pour incrémenter le nombre présent dans le Fichier X. Ainsi, l'appareil et la procédure de l'invention rendent vain un copiage non autorisé.

En outre, en cas d'altération de l'appareil spécial 12 mettant cet appareil hors fonction, le disque original devient inutilisable, du fait que le Fichier X ne peut pas être incrémenté sans l'utilisation de l'appareil spécial.

Comme le montre la figure, l'appareil spécial 12, comprend, dans le mode de réalisation représenté, une tête de lecture/écriture 20, un amplificateur 22, un dispositif d'augmentation et d'enregistrement 24, et une batterie 26 qui alimente les autres composants. L'ensemble de cet appareil spécial 12 est monté dans la pochette du disque. La tête de lecture/écriture 20 est extrêmement mince et est positionnée sur la pochette dans une position fixe telle qu'elle ne puisse accéder qu'à la piste

de sécurité spécialisée 14 sur le disque 16.

On suppose à titre d'exemple que la piste 14 du disque 16 qui est spécialisé pour la sécurité est la Piste 3. L'appareil spécial de la figure fonctionne de la manière suivante.

Lorsque l'ordinateur reçoit l'ordre de lire le programme sur le disque 16, il fait démarrer la rotation du disque 16. Pendant le premier tour, la tête de lecture/écriture 20 du disque détecte une impulsion de synchronisation initiale sur la Piste 3, c'est-à-dire la piste spécialisée 14. On utilise cette impulsion de synchronisation pour mettre en fonction l'amplificateur 22 et le dispositif d'augmentation et d'enregistrement 24.

Le disque 16 continuant à tourner, la tête de lecture/écriture 20 du disque lit un nombre N_o qui suit la première impulsion de synchronisation sur la Piste 3. Ce nombre N_o est incrémenté d'un nombre enregistré dans le dispositif d'augmentation et d'enregistrement 24, pour donner un nombre incrémenté N_1.

Pendant le second tour du disque 16, la tête de lecture/écriture 20 du disque détecte à nouveau l'impulsion de synchronisation. Cette seconde impulsion de synchronisation commute l'amplificateur 22 de façon à transmettre le nombre N_1 au disque 16 dans lequel N_1 est écrit sur N_o dans la Piste 3. Le dispositif d'augmentation et d'enregistrement 24 fait en sorte que l'amplificateur 22 ignore toute les impulsions de synchronisation supplémentaires qui peuvent être lues par la suite. Le répertoire du système d'exploitation affecte un nom à la Piste 3 : la Piste 3 est le Fichier X.

Comme décrit ci-dessus, le programme comprend une procédure de contrôle de sécurité dans laquelle un nombre N_o, enregistré en langage machine dans le sous-programme d'initialisation, est incrémenté de la même

manière que précédemment, pour produire le nombre N_1 dans un Fichier Y. Le sous-programme d'initialisation compare ensuite le nombre dans le Fichier X avec le nombre dans le Fichier Y. Si le nombre dans le Fichier X est égal au nombre dans le Fichier Y, les données protégées sont transférées vers la mémoire centrale de l'ordinateur, par la tête de lecture/écriture 18 de l'ordinateur. Si le nombre dans le Fichier X n'est pas égal au nombre dans le Fichier Y, la procédure de contrôle de sécurité ordonne à la tête de lecture/écriture 18 de l'ordinateur d'emplir tous les fichiers, y compris ceux contenant les données protégées, avec des nombres dépourvus de signification.

Dans la forme la plus simple de ce mode de réalisation, les nombres contenus dans les Fichiers X et Y sont incrémentés de la même quantité chaque fois que le disque est lu. Dans une version légèrement plus complexe, la valeur de l'incrément change chaque fois que le disque est lu. On peut effectuer ceci en modifiant un nombre enregistré dans un fichier d'incrément spécial chaque fois que le disque est lu.

On a ainsi décrit trois modes de réalisation d'un procédé et d'un appareil destinés à déjouer le copiage non autorisé de données protégées qui ont été enregistrées sur un disque souple. On voit clairement que le procédé et l'appareil sont adaptables à d'autres supports d'enregistrement.

Dans chaque mode de réalisation, un disque autorisé reçoit une empreinte digitale qui permet de distinguer physiquement ce disque d'un disque ordinaire sur lequel serait réalisée une copie non autorisée.

Dans le premier mode de réalisation, l'empreinte digitale consiste en une zone défectueuse introduite intentionnellement, ayant une position aléatoire. Dans le second mode de réalisation, l'empreinte digitale consis-

te en une signature magnétique inaltérable qui est enregistrée sur une partie spéciale du disque, permettant uniquement la lecture. Dans le troisième mode de réalisation, l'empreinte digitale est une signature magnétique qui est enregistrée sur une piste spécialisée du disque et qui est modifiée chaque fois que le disque est utilisé.

Dans chaque mode de réalisation, le sous-programme d'initialisation enregistré sur le disque contient une procédure de contrôle de sécurité qui effectue un test portant sur la présence de l'empreinte digitale connue, et qui empêche la lecture des données protégées si l'empreinte digitale est absente, comme ce serait le cas pour une copie non autorisée.

Il va de soi que de nombreuses modifications peuvent être apportées à l'appareil et au procédé décrits et représentés, sans sortir du cadre de l'invention.

REVENDICATIONS

1. Procédé pour déjouer le copiage non autorisé de données protégées qui ont été enregistrées sur un support et qui sont lues sur le support par un appareil qui est commandé par des instructions enregistrées sur le support, ces instructions faisant partie d'un sous-programme d'initialisation qui est exécuté avant la lecture des données protégées sur le support, caractérisé en ce qu'il comprend les opérations suivantes : (a) on place des marques distinctives dans le support de copies autorisées, en sachant que ces marques distinctives sont absentes des supports dans lesquels on enregistre des copies non autorisées ; (b) on effectue un test pour déterminer si les marques distinctives sont présentes dans une copie utilisée, celle-ci pouvant être une copie autorisée ou une copie non autorisée; et (c) on interdit la lecture des données protégées si le test indique que les marques distinctives sont absentes de la copie qui est utilisée.

2. Procédé selon la revendication 1, caractérisé en ce que l'opération (c) comprend en outre l'effacement des données protégées si le test indique que les marques distinctives sont absentes de la copie utilisée.

3. Procédé pour déjouer le copiage non autorisé de données protégées qui ont été enregistrées dans un support et qui sont lues sur le support par un appareil qui est commandé par des instructions enregistrées dans le support, ces instructions faisant partie d'un sous-programme d'initialisation qui est exécuté avant la lecture des données protégées sur le support, caractérisé en ce qu'il comprend les opérations suivantes : (a) on crée intentionnellement une zone défectueuse permanente localisée dans le support, avant l'enregistrement des données protégées, la zone défectueuse étant incapable d'enregistrer des données et

la zone défectueuse se trouvant à une position aléatoire sur une partie du support réservée aux données protégées; (b) on détermine la position de la zone défectueuse dans le support; (c) on enregistre la position de la zone défectueuse dans le sous-programme d'initialisation ; (d) on écrit des données particulières à la position de la zone défectueuse ; (e) on lit les données qui ont pu être enregistrées à la position de la zone défectueuse; (f) on compare les données lues à l'opération (e) avec les données écrites à l'opération (d); et (g) on interdit la lecture des données protégées si les données lues à l'opération (e) sont identiques aux données écrites à l'opération (d).

4. Support destiné à l'enregistrement de données protégées, ce support contenant également un sous-programme d'initialisation qui est exécuté avant que les données protégées ne soient lues sur le support, et qui commande un appareil destiné à lire des données sur le support et à enregistrer des données sur le support, caractérisé en ce qu'il comprend un défaut permanent localisé, produit intentionnellement, qui se trouve dans une partie du support qui est réservée aux données protégées, à une position aléatoire qui est enregistrée dans le sous-programme d'initialisation, grâce à quoi on reconnaît une copie non autorisée si le sous-programme d'initialisation parvient à lire sous une forme identique des données dont le sous-programme d'initialisation a commandé l'écriture à la position enregistrée du défaut.

5. Procédé pour déjouer le copiage non autorisé de données protégées enregistrées dans un support qui comprend une partie spéciale permettant uniquement la lecture, dans laquelle un nombre constituant une empreinte digitale permanente a été enregistré de façon inaltérable, ce support contenant également un sous-

programme d'initialisation qui est exécuté avant la lecture des données protégées sur le support, et qui commande le fonctionnement de la tête de lecture/écriture qui dessert le support, caractérisé en ce qu'il comprend les opérations suivantes : (a) on établit un fichier à la position à laquelle se trouve la partie spéciale, permettant uniquement la lecture, d'une copie autorisée; (b) on ordonne à la tête de lecture/écriture d'écrire dans le fichier un nombre de test qui est différent du nombre constituant une empreinte digitale; puis (c) on lit le contenu du fichier ; (d) on compare le contenu du fichier avec le nombre de test; et (e) on interdit la lecture des données protégées si le contenu du fichier est identique au nombre de test.

6. Support destiné à l'enregistrement de données, ce support étant normalement utilisé en association avec un appareil standard qui peut lire, écrire et effacer sélectivement des données dans le support, caractérisé en ce qu'il comprend une partie dans laquelle un appareil spécial peut écrire des données spéciales, et dans laquelle l'appareil standard ne peut pas effacer les données spéciales.

7. Procédé pour déjouer le copiage non autorisé de données protégées qui ont été enregistrées dans un support autorisé qui contient un sous-programme d'initialisation qui est exécuté avant que les données protégées ne soient lues dans le support autorisé, caractérisé en ce qu'il comprend les opérations suivantes : (a) on établit un Fichier X; (b) on enregistre initialement un nombre particulier N_o dans le Fichier X ; (c) on établit un appareil d'augmentation (12) qui n'existe que lorsqu'on utilise un support autorisé, destiné à produire une série d'incréments et à incrémenter successivement le nombre présent dans le Fichier X, chaque fois que le support est lu, cet appareil d'augmentation étant absent lorsqu'on utilise

un support non autorisé et cessant de fonctionner lorsqu'un support autorisé a été altéré; (d) on établit un Fichier Y dans le sous-programme d'initialisation; (e) on enregistre initialement dans le Fichier Y le nombre N_o utilisé à l'opération (b); (f) on incrémente successivement le nombre présent dans le Fichier Y, à chaque lecture du support, conformément à une série d'incréments identique à celle qui a été établie à l'opération (c); (g) on effectue un test pour déterminer si le nombre présent dans le Fichier X est égal au nombre présent dans le Fichier Y; et (h) on interdit la lecture des données protégées si le nombre présent dans le Fichier X n'est pas égal au nombre présent dans le Fichier Y.

8. Appareil destiné à déjouer le copiage non autorisé de données protégées qui ont été enregistrées dans cet appareil en compagnie d'un sous-programme d'initialisation qui est exécuté avant que les données protégées ne soient lues,ce sous programme d'initialisation comprenant des instructions destinées à produire une série d'incréments et à incrémenter successivement un premier nombre enregistré dans le sous-programme d'initialisation, chaque fois que l'appareil est utilisé, caractérisé en ce qu'il comprend : un support d'enregistrement (16); et des moyens d'augmentation (12) associés au support d'enregistrement de façon à enregistrer une seconde série d'incréments, identique à la première série d'incréments, et à incrémenter successivement un second nombre égal au premier nombre et enregistré dans un fichier particulier (14) du support d'enregistrement (16), chaque fois que le support est lu, grâce à quoi le sous-programme d'initialisation peut reconnaître à temps une copie non autorisée, qui est dépourvue des moyens d'augmentation, pour interdire la lecture des données protégées sous l'effet de toute inégalité entre des incréments successifs du premier nombre et des incréments successifs correspondants du second nombre.

2535885

