ROYAUME DU MAROC

OFFICE MAROCAIN DE LA PROPRIETE INDUSTRIELLE ET COMMERCIALE
---

(19)

المملكة المغربية
المكتب المغربي للملكية الصناعية و التجارية

(12) BREVET D'INVENTION

(11) N° de publication :
MA 53262 B1

(51) Cl. internationale :
H04L 9/32; H04L 9/00

(43) Date de publication :
31.05.2024

(21) N° Dépôt :
53262

(22) Date de Dépôt :
15.07.2019

(30) Données de Priorité :
06.08.2018 EP 18187473

(86) Données relatives à la demande internationale selon le PCT:
PCT/EP2019/068986 15.07.2019

(71) Demandeur(s) :
SICPA HOLDING SA, Avenue de Florissant 41 1008 Prilly (CH)

(72) Inventeur(s) :
DECOUX, Eric ; THEVOZ, Philippe ; WALLACE, Elisabeth ; GILLET, Philippe

(74) Mandataire :
CABINET DIANI

(54) Titre : **PROTECTION ANTI-FALSIFICATION DE FICHIER NUMÉRIQUE**

(57) Abrégé : L'invention concerne la sécurisation d'un fichier numérique original contre la falsification et la falsification de ses données associées, et en particulier de données relatives à son appartenance à un lot spécifique de fichiers numériques originaux, tout en permettant une vérification hors ligne ou en ligne de l'authenticité d'un fichier numérique sécurisé et la conformité de ses données associées par rapport à celle d'un fichier numérique original authentique. L'invention est particulièrement utile pour sécuriser des fichiers numériques prêts à l'impression.

REVENDICATIONS

1. Procédé de protection d'un fichier numérique original (A_1, …, A_8) donné apparentant à un lot d'une pluralité de fichiers numériques originaux (A_1, …, A_8) contre la contrefaçon ou la falsification, chaque fichier numérique original (A_1, …, A_8) comportant ses propres données numériques (D_1, …, D_8), comprenant les étapes suivantes :

pour chaque fichier numérique original (A_1, …, A_8) du lot, le calcul, au moyen d'une fonction unidirectionnelle (H), d'une signature de fichier numérique (x_1, …, x_8) associée de ses données numériques (D_1, …, D_8) ;

la formation d'un arbre sur la base de la pluralité de signatures de fichier numérique (x_1, …, x_8) calculées pour les fichiers numériques originaux (A_1, …, A_8) du lot et comprenant des nœuds agencés selon un ordre de nœuds donné dans l'arbre, ledit arbre comprenant des niveaux de nœud, des nœuds feuille, correspondant à la pluralité de signatures de fichier numérique (x_1, …, x_8) respectivement associées à la pluralité de fichiers numériques originaux (A_1, …, A_8) dans le lot, au nœud racine de l'arbre, chaque nœud non feuille de l'arbre correspondant à une signature numérique au moyen de la fonction unidirectionnelle d'une concaténation des signatures numériques respectives de ses nœuds enfant selon un ordre de concaténation d'arbre, le nœud racine correspondant à une signature numérique racine de référence (R), c'est-à-dire une signature numérique au moyen de la fonction unidirectionnelle d'une concaténation des signatures numériques des nœuds d'un avant-dernier niveau de nœuds dans l'arbre selon ledit ordre de concaténation d'arbre ;

l'association, avec le fichier numérique original (A_1, …, A_8) donné, d'une clé de vérification numérique (k_1, … k_8)

correspondante étant une séquence des signatures numériques respectives, à partir du niveau de nœuds feuille jusqu'au niveau des avant-derniers nœuds, de chaque autre nœud feuille ayant le même nœud parent dans l'arbre que le nœud feuille correspondant à la signature de fichier numérique (x_1, …, x_8) du fichier numérique original (A_1, …, A_8) donné, et successivement à chaque niveau suivant dans l'arbre, de chaque nœud non-feuille ayant le même nœud parent dans l'arbre que le même nœud parent précédent considéré au niveau précédent ;

la mise à la disposition d'un utilisateur de la signature numérique racine de référence (R) de l'arbre ; et caratérisé par

l'inclusion, dans le fichier numérique original (A_1, …, A_8) donné, d'un marquage de sécurité numérique lisible par machine (110) correspondant comprenant une représentation de ses données numériques (D_1, …, D_8) et de sa clé de vérification numérique (k_1, … k_8) correspondante,

ce qui permet d'obtenir un fichier numérique original (A_1, …, A_8) marqué dont les données numériques (D_1, …, D_8) sont protégées contre la contrefaçon ou la falsification.

2. Procédé selon la revendication 1, dans lequel la signature numérique racine de référence (R) du nœud racine de l'arbre est soit publiée sur un support accessible à l'utilisateur, soit stockée dans une base de données racine consultable accessible à l'utilisateur, soit stockée dans une chaîne de blocs ou dans une base de données protégée par une chaîne de blocs, accessible à l'utilisateur.

3. Procédé selon la revendication 1 ou la revendication 2, dans lequel

un fichier numérique virtuel est compté comme appartenant au lot de fichiers numériques originaux (A_1, …, A_8), ledit fichier numérique virtuel comportant ses propres données numériques virtuelles, et une signature de fichier numérique virtuel associée obtenue au moyen de la fonction unidirectionnelle (H) des données numériques virtuelles, ledit fichier numérique virtuel n'étant pas réel mais uniquement utilisé pour générer la signature de fichier numérique virtuel associée à partir de ses données numériques virtuelles ; et

la signature numérique racine de référence (R) associée audit lot de fichiers numériques originaux (A_1, …, A_8) étant calculée à partir d'un arbre ayant toutes les signatures de fichiers numériques des fichiers numériques originaux (A_1, …, A_8) du lot, dont la signature de fichier numérique virtuel, en tant que nœuds feuille.

4. Procédé selon l'une quelconque des revendications 1 à 3, dans lequel

des données numériques additionnelles correspondant aux données numériques (D_1, …, D_8) associées au fichier numérique original (A_1, …, A_8) marqué sont stockées dans une base de données d'informations consultable accessible à l'utilisateur via une interface de base de données d'informations servant à recevoir, en provenance de l'utilisateur, une requête d'informations contenant des données numériques (D_1, …, D_8), ou une signature de fichier numérique (x1, …, x_8), obtenue à partir d'un marquage de sécurité numérique (110) d'un fichier numérique original (A_1, …, A_8) marqué, et renvoyer des données numériques additionnelles correspondantes.

5. Procédé selon l'une quelconque des revendications 1 à 4, dans lequel les données numériques (D_1, …, D_8) du fichier

numérique original (A_1, …, A_8) marqué comportent des données numériques de caractéristique de référence d'une caractéristique physique unique correspondante d'un objet ou d'un individu associé.

6. Procédé selon l'une quelconque des revendications 1 à 5, dans lequel les données numériques (D_1, …, D_8) des fichiers numériques originaux (A_1, …, A_8) respectifs du lot sont réparties entre des champs donnés communs à tous les fichiers numériques du lot, et des données numériques spécifiques relatives à ces champs ne sont pas incluses dans les données numériques (D_1, …, D_8) mais regroupées dans un bloc de données de champs séparé associé au lot, et dans lequel :

i) la signature de fichier numérique (x_1, …, x_8) d'un fichier numérique original (A_1, …, A_8) est calculée avec la fonction unidirectionnelle d'une concaténation des données numériques (D_1, …, D_8) correspondantes et du bloc de données de champs ; et

ii) la signature numérique racine de référence (R) est mise à la disposition de l'utilisateur avec le bloc de données de champs associé.

7. Procédé de vérification de l'authenticité d'un fichier numérique protégé selon le procédé de l'une quelconque des revendications 1 à 5, ou de la conformité d'une copie d'un tel fichier numérique protégé par rapport à l'original, caractérisé en ce qu'il comprend, lors du traitement d'un fichier test qui est ledit fichier numérique ou ladite copie du fichier numérique au moyen d'une unité de traitement connectée à une mémoire, les étapes suivantes :

le fait de posséder, stocké dans la mémoire, le fichier de test ;

la lecture d'une représentation de données numériques (D_1, …, D_8) et d'une clé de vérification numérique (k_1, … k_8) sur un marquage de sécurité numérique (110) du fichier de test stocké, et l'extraction de données numériques de test respectivement correspondantes et d'une clé de vérification numérique de test respectivement correspondante à partir de ladite représentation lue ;

le fait de posséder, stockée dans la mémoire, une signature numérique racine de référence (R) d'un nœud racine d'un arbre du lot de fichiers numériques originaux (A_1, …, A_8), et ayant, programmée dans l'unité de traitement, la fonction unidirectionnelle (H) pour calculer une signature numérique de données numériques (D_1, …, D_8) et d'une concaténation de signatures numériques selon l'ordre de nœuds dans l'arbre et de l'ordre de concaténation d'arbre ;

la vérification de si les données numériques de test extraites et la clé de vérification numérique de test associée correspondent effectivement à la signature numérique racine de référence (R) stockée par la réalisation des étapes suivantes :

le calcul, avec la fonction unidirectionnelle, d'une signature numérique de test des données numériques de test extraites, ladite signature numérique de test correspondant à un nœud feuille de test dans un arbre de test correspondant au marquage de sécurité numérique (110) du fichier de test ;

l'extraction, à partir de la séquence de signatures numériques dans la clé de vérification numérique de test, d'une signature numérique de chaque autre nœud feuille de l'arbre de test ayant le même nœud parent que celui du nœud feuille de test et le calcul d'une signature numérique d'une concaténation de la signature numérique de test et de la signature numérique extraite dudit

chaque autre nœud feuille, en obtenant ainsi une signature numérique dudit même nœud parent du nœud feuille de test ;

successivement, à chaque niveau suivant dans l'arbre de test et jusqu'à l'avant-dernier niveau de nœuds, l'extraction, à partir de la séquence de signatures numériques dans la clé de vérification numérique de test, d'une signature numérique de chaque autre nœud non-feuille de l'arbre de test ayant le même nœud parent que celui du même nœud parent précédent pris en considération à l'étape précédente et le calcul d'une signature numérique d'une concaténation de la signature numérique dudit chaque autre nœud non-feuille respectif et de la signature numérique obtenue dudit même nœud parent précédent, en obtenant ainsi une signature numérique dudit même nœud parent dudit même nœud parent précédent ;

le calcul d'une signature numérique d'une concaténation des signatures numériques obtenues des nœuds non-feuille correspondant à l'avant-dernier niveau de nœuds de l'arbre de test, en obtenant ainsi une signature numérique racine candidate du nœud racine de l'arbre de test ; et

le contrôle de si la signature numérique racine candidate obtenue concorde avec la signature numérique racine de référence (R) stockée,

moyennant quoi, dans le cas où lesdites signatures numériques racines concordent, les données numériques (D_1, …, D_8) du fichier de test sont celles d'un fichier numérique authentique.

8. Procédé selon la revendication 7, dans lequel le fichier numérique original (A_1, …, A_8) marqué est protégé selon le procédé de la revendication 6, la mémoire de l'unité de

traitement stockant en outre le bloc de données de champs associé, et dans lequel :

l'étape de calcul d'une signature numérique de test correspondant à un nœud feuille de test dans un arbre de test correspondant au marquage de sécurité numérique (110) sur le fichier de test comprend le calcul, avec la fonction unidirectionnelle, d'une signature numérique d'une concaténation des données numérique de test extraites et du bloc de données de champs stocké.

9. Procédé selon l'une quelconque des revendications 7 et 8, dans lequel le fichier numérique est protégé par le stockage de la signature numérique racine de référence (R) dans une base de données racine consultable accessible à l'utilisateur selon le procédé de la revendication 2, et l'unité de traitement est en outre connectée à une unité de communication servant à envoyer et recevoir en retour des données via une liaison de communication, comprenant les étapes préliminaires de :

l'envoi, avec l'unité de communication via la liaison de communication, d'une requête à ladite base de données racine, et la réception en retour de la signature numérique racine de référence (R) ; et

le stockage de la signature numérique racine reçue dans la mémoire de la mémoire.

10. Procédé selon l'une quelconque des revendications 7 à 9, dans lequel le fichier numérique est protégé selon le procédé de la revendication 4 et l'imageur est en outre équipé de moyens de communication servant à envoyer, à l'interface de base de données d'informations, une requête d'informations contenant des données numériques (D_1, …, D_8), ou une signature de fichier numérique (x_1, …, x_8), obtenue à partir

du marquage de sécurité numérique (110) du fichier de test, et recevoir en retour des données numériques additionnelles correspondantes.

11. Procédé selon l'une quelconque des revendications 7 à 10, dans lequel l'imageur est en outre équipé d'un capteur servant à détecter une caractéristique physique unique respectivement d'un objet ou d'un individu associé, et l'unité de traitement est programmée pour extraire des données numériques de caractéristique correspondantes à partir d'un signal de détection reçu en provenance du capteur, l'imageur ayant, stockées dans la mémoire, des données numériques de caractéristique CDD de référence correspondant à ladite caractéristique physique unique respectivement de l'objet ou de l'individu associé, comprenant les étapes supplémentaires de, lors de la visualisation d'un sujet qui est ledit objet ou individu associé :

la détection, avec le capteur, d'une caractéristique physique unique du sujet et l'extraction de données numériques de caractéristique candidates CDD^c correspondantes ;

la comparaison des données numériques de caractéristique candidates CDD^c obtenues avec les données numériques de caractéristique CDD de référence stockées ; et

dans le cas où les données numériques de caractéristique candidates CDD^c sont similaires aux données numériques de caractéristique CDD de référence stockées, dans les limites d'un critère de tolérance donné, le sujet est considéré comme correspondant respectivement à un objet ou individu authentique associé de manière valide à un fichier numérique authentique.

12. Fichier numérique appartenant à un lot d'une pluralité de fichiers numériques originaux (A_1, …, A_8) et protégé selon le procédé de l'une quelconque des revendications 1 à 6, chaque fichier numérique original (A_1, …, A_8) du lot ayant ses propres données numériques (D_1, …, D_8) et clé de vérification numérique (k_1, … k_8) correspondante, ledit lot ayant une signature numérique racine de référence (R) correspondante, comprenant :

un marquage de sécurité lisible par machine comportant une représentation de ses données numériques (D_1, …, D_8) et de sa clé de vérification.

13. Système pour la vérification de l'authenticité d'un fichier numérique, ou de la conformité d'une copie d'un tel fichier numérique, par rapport à un fichier numérique original (A_1, …, A_8) marqué appartenant à un lot de fichiers numériques originaux (A_1, …, A_8) protégés selon le procédé de l'une quelconque des revendications 1 à 5, comprenant un imageur ayant une unité d'imagerie, une unité de traitement dotée d'une mémoire, et une unité de traitement d'image, la mémoire stockant une signature numérique racine de référence (R) d'un arbre correspondant au lot de fichiers numériques originaux (A_1, …, A_8), et la fonction unidirectionnelle (H) pour calculer une signature numérique de données numériques (D_1, …, D_8) et d'une concaténation de signatures numériques selon l'ordre de nœuds de l'arbre et l'ordre de concaténation d'arbre qui sont programmés dans l'unité de traitement, ledit système servant à :

posséder, stocké dans la mémoire, un fichier de test qui est ledit fichier numérique ou ladite copie du fichier numérique ;

lire une représentation de données numériques (D_1, …, D_8) et d'une clé de vérification numérique (k_1, … k_8) sur un

marquage de sécurité numérique (110) du fichier de test stocké, et extraire des données numériques de test respectivement correspondantes et une clé de vérification numérique de test respectivement correspondante à partir de ladite représentation lue ;

vérifier que les données numériques de test extraites et la clé de vérification numérique de test extraite correspondent effectivement à la signature numérique racine de référence (R) stockée par la réalisation, sur l'unité de traitement, des opérations programmées de :

le calcul, avec la fonction unidirectionnelle, d'une signature numérique de test des données numériques de test extraites, ladite signature numérique de test correspondant à un nœud feuille de test dans un arbre de test correspondant au marquage de sécurité numérique (110) du fichier de test ;

l'extraction, à partir de la séquence de signatures numériques dans la clé de vérification numérique de test, d'une signature numérique de chaque autre nœud feuille de l'arbre de test ayant le même nœud parent que celui du nœud feuille de test et le calcul d'une signature numérique d'une concaténation de la signature numérique de test et de la signature numérique extraite dudit chaque autre nœud feuille, en obtenant ainsi une signature numérique dudit même nœud parent du nœud feuille de test ;

successivement, à chaque niveau suivant dans l'arbre de test et jusqu'à l'avant-dernier niveau de nœuds, l'extraction, à partir de la séquence de signatures numériques dans la clé de vérification numérique de test, d'une signature numérique de chaque autre nœud non-feuille de l'arbre de test ayant le même nœud parent que celui du même nœud parent précédent pris en considération

à l'étape précédente et le calcul d'une signature numérique d'une concaténation de la signature numérique dudit chaque autre nœud non-feuille respectif et de la signature numérique obtenue dudit même nœud parent précédent, en obtenant ainsi une signature numérique dudit même nœud parent dudit même nœud parent précédent ;

le calcul d'une signature numérique d'une concaténation des signatures numériques obtenues des nœuds non-feuille correspondant à l'avant-dernier niveau de nœuds de l'arbre de test, en obtenant ainsi une signature numérique racine candidate du nœud racine de l'arbre de test ; et

le contrôle de si la signature numérique racine candidate obtenue concorde avec la signature numérique racine de référence (R) stockée,

moyennant quoi, dans le cas où lesdites signatures numériques racines concordent, le système est configuré pour fournir une indication selon laquelle les données numériques du fichier de test sont celles d'un fichier numérique authentique.

14. Système selon la revendication 13, dans lequel le fichier numérique original (A_1, …, A_8) marqué est protégé selon le procédé de la revendication 6, la mémoire de l'unité de traitement stockant en outre le bloc de données de champs associé, et dans lequel :

les opérations programmées de calcul d'une signature numérique de test correspondant à un nœud feuille de test dans un arbre de test correspondant au marquage de sécurité numérique (110) du fichier de test comprennent le calcul, avec la fonction unidirectionnelle, d'une signature numérique d'une concaténation des données numérique de test extraites et du bloc de données de champs stocké.

15. Système selon l'une quelconque des revendications 13 et 14, dans lequel le fichier numérique original (A_1, …, A_8) marqué appartient à un lot de fichiers numériques originaux (A_1, …, A_8) protégés selon le procédé de la revendication 5, le système étant en outre équipé d'un capteur connecté à l'unité de traitement et servant à détecter une caractéristique physique unique d'un objet ou d'un individu associé, et l'unité de traitement étant programmée pour extraire des données numériques de caractéristique correspondantes à partir d'un signal de détection reçu en provenance du capteur, le système ayant, stockées dans la mémoire, des données numériques de caractéristique CDD de référence correspondant à ladite caractéristique physique unique de l'objet ou de l'individu associé, le système servant en outre à :

détecter, avec le capteur, une caractéristique physique unique d'un sujet qui est ledit objet ou individu associé, et extraire des données numériques de caractéristique candidates CDD^c correspondantes ;

comparer les données numériques de caractéristique candidates CDD^c obtenues avec les données numériques de caractéristique CDD de référence stockées ; et

dans le cas où les données numériques de caractéristique candidates CDD^c sont similaires aux données numériques de caractéristique CDD de référence stockées, dans les limites d'un critère de tolérance donné, fournir une indication selon laquelle le sujet est considéré comme étant authentique.