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 58214 B1

(51) Cl. internationale :
B42D 25/24

(43) Date de publication :
30.11.2022

(21) N° Dépôt :
58214

(22) Date de Dépôt :
03.06.2019

(30) Données de Priorité :
10.07.2018 EP 20180182697

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

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

(74) Mandataire :
CABINET DIANI

(86) N° de dépot auprès de l'organisme de validation: EP19727044.0

(54) Titre : **PROTECTION ANTICONTREFAÇON D'ARTICLES**

(57) Abrégé : L'invention concerne la sécurisation d'un article contre la contrefaçon et la falsification de ses données associées, et en particulier de données relatives à son appartenance à un lot spécifique d'articles, tout en permettant une vérification hors ligne ou en ligne de l'authenticité d'un article sécurisé et de la conformité de ses données associées par rapport à celles d'un article authentique.

REVENDICATIONS

1. Procédé de sécurisation d'un article d'origine donné appartenant à un lot d'une pluralité d'articles d'origine (A_1,…,A_8) contre la contrefaçon ou l'altération, chaque article d'origine ayant ses propres données d'article associées et des données numériques d'article (D_1,…,D_8) correspondantes, le procédé comprenant les étapes de :

pour chaque article d'origine du lot, calcul au moyen d'une fonction unidirectionnelle (H) d'une signature numérique d'article (x_1,…,x_8) associée de ses données numériques d'article correspondantes ;

formation d'un arbre sur la base de la pluralité de signatures numériques d'article calculées pour les articles d'origine du lot et comprenant des nœuds agencés selon un ordonnancement donné des nœuds dans l'arbre, ledit arbre comprenant des niveaux de nœud des nœuds feuilles (a(1,1),…,a(1,8)), correspondant à la pluralité de signatures numériques d'article respectivement associées à la pluralité d'articles d'origine dans le lot, au nœud racine (R) de l'arbre, chaque nœud non-feuille (a(2,1),…,a(2,4), a(3,1), a(3,2)) de l'arbre correspondant à une signature numérique au moyen de la fonction unidirectionnelle d'une concaténation des signatures numériques respectives de ses nœuds enfants selon un ordonnancement de concaténation d'arbre, le nœud racine correspondant à une signature numérique racine de référence, à savoir une signature numérique au moyen de la fonction unidirectionnelle d'une concaténation des signatures numériques des nœuds (a(3,1), a(3,2)) d'un niveau de nœuds pénultièmes dans l'arbre selon ledit ordonnancement de concaténation d'arbre ;

association avec l'article d'origine donné d'une clé de vérification correspondante étant une séquence des signatures numériques respectives, du niveau de nœuds feuilles au niveau de nœuds pénultièmes, de chaque autre nœud feuille ayant le même nœud parent dans l'arbre que le nœud feuille correspondant à la signature numérique d'article de l'article d'origine 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 antérieur considéré au niveau précédent ;

mise à disposition d'un utilisateur de la signature numérique racine de référence de l'arbre ; et

application sur l'article d'origine donné d'un marquage de sécurité lisible par machine (110) incluant une représentation de ses données numériques d'article correspondantes et sa clé de vérification correspondante,

pour ainsi obtenir un article d'origine marqué dont les données d'article sont sécurisées contre la contrefaçon ou l'altération.

2. Procédé selon revendication 1, dans lequel la signature numérique racine de référence du nœud racine de l'arbre est soit publiée dans 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 (260), ou dans une base de données sécurisée par une chaîne de blocs, accessible à l'utilisateur.

3. Procédé selon revendication 2, dans lequel l'article d'origine marqué comprend en outre des données d'accès au nœud racine marquées sur celui-ci et contenant des informations suffisantes pour permettre à l'utilisateur d'accéder à la signature numérique racine de référence du

nœud racine de l'arbre correspondant au lot d'articles d'origine, lesdites informations étant un lien à une interface d'accès servant à recevoir à partir de l'utilisateur une requête racine contenant des données numériques d'article, ou une signature numérique de données numériques d'article, obtenues à partir d'un marquage de sécurité d'un article d'origine marqué, et à renvoyer une signature numérique racine de référence d'arbre correspondant, l'interface d'accès permettant l'accès, respectivement, à l'un des suivants :

- le support dans lequel la signature numérique racine de référence est publiée ;
- la base de données racine consultable dans laquelle la signature numérique racine de référence est stockée ; et
- la chaîne de blocs, ou respectivement la base de données sécurisée par une chaîne de blocs, dans laquelle la signature numérique racine de référence à estampille temporelle est stockée.

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

un article virtuel est compté comme appartenant au lot d'articles d'origine, ledit article virtuel ayant des données d'article virtuel associées et ses données numériques d'article virtuel correspondantes, et une signature numérique d'article virtuel associée obtenue au moyen de la fonction unidirectionnelle des données numériques d'article virtuel, ledit article virtuel n'étant pas produit mais seulement utilisé pour générer la signature numérique d'article virtuel associée ; et

la signature numérique racine de référence associée audit lot d'articles d'origine étant calculée à partir d'un arbre ayant toutes les signatures numériques d'article des articles

d'origine du lot, incluant la signature numérique d'article virtuel, en tant que nœuds feuilles.

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

des données numériques d'article additionnelles correspondant aux données numériques d'article associées à l'article d'origine marqué sont stockées dans une base de données d'informations (250) consultable accessible à l'utilisateur par l'intermédiaire d'une interface de base de données d'informations servant à recevoir à partir de l'utilisateur une requête d'informations contenant des données numériques d'article, ou une signature numérique de données numériques d'article, obtenues à partir d'un marquage de sécurité d'un article d'origine marqué, et à renvoyer les données numériques d'article additionnelles correspondantes.

6. Procédé selon revendication 5, dans lequel les données numériques d'article additionnelles correspondant aux données numériques d'article associées à l'article d'origine marqué sont concaténées avec lesdites données numériques d'article.

7. Procédé selon l'une quelconque des revendications 1 à 6, dans lequel les données numériques d'article de l'article d'origine marqué incluent des données numériques de caractéristique de référence correspondantes d'une caractéristique physique unique de l'article d'origine marqué, ou d'un objet ou individu associé, dans lequel la caractéristique physique unique de l'article d'origine marqué est de préférence celle d'un marquage de sécurité matériel appliqué sur l'article d'origine, ou sur l'objet associé.

8. Procédé selon l'une quelconque des revendications 1 à 7, dans lequel les données numériques d'article des articles d'origine respectifs du lot sont propagées entre des champs donnés communs à tous les articles du lot, et les données numériques relatives à ces champs ne sont pas incluses dans les données numériques d'article mais regroupées dans un bloc de données de champs séparé associé au lot, et dans lequel :

i) la signature numérique d'article d'un article d'origine est calculée avec la fonction unidirectionnelle d'une concaténation des données numériques d'article correspondantes et des données numériques du bloc de données de champs ; et

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

9. Procédé de vérification de l'authenticité d'un article, ou de la conformité d'une copie d'un tel article, ou de la conformité d'une image numérique d'article d'un tel article, par rapport à un article d'origine marqué appartenant à un lot d'articles d'origine sécurisés selon le procédé selon l'une quelconque des revendications 1 à 7, le procédé comprenant les étapes de :

acquisition d'une image numérique d'un marquage de sécurité sur un objet de test étant ledit article ou ladite copie de l'article, ou obtention de l'image numérique d'article montrant un marquage de sécurité sur l'article, au moyen d'un imageur ayant une unité d'imagerie, une unité de traitement comportant une mémoire, et une unité de traitement d'image ;

lecture d'une représentation de données numériques d'article et d'une clé de vérification associée sur l'image numérique acquise du marquage de sécurité sur l'objet de

test, et extraction respective de données numériques d'article de test correspondantes et d'une clé de vérification de test à partir de ladite représentation lue ;

ayant, stockée dans la mémoire, une signature numérique racine de référence d'un nœud racine d'un arbre du lot d'articles d'origine, et ayant programmée dans l'unité de traitement la fonction unidirectionnelle pour calculer une signature numérique de données numériques et d'une concaténation de signatures numériques selon l'ordonnancement des nœuds dans l'arbre et l'ordonnancement de concaténation d'arbre ;

fait de vérifier si les données numériques d'article de test extraites et la clé de vérification de test associée correspondent bien à la signature numérique racine de référence stockée en réalisant les étapes de :

calcul avec la fonction unidirectionnelle d'une signature numérique de test des données numériques d'article 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 sur l'objet de test ;

extraction à partir de la séquence de signatures numériques dans la clé de vérification 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 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, pour ainsi obtenir une signature numérique dudit même nœud parent du nœud feuille de test ;

successivement à chaque niveau suivant dans l'arbre de test et jusqu'au niveau de nœuds pénultièmes, extraction à partir de la séquence de signatures

numériques dans la clé de vérification 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 antérieur considéré à l'étape précédente et 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 antérieur, pour ainsi obtenir une signature numérique dudit même nœud parent dudit même nœud parent antérieur ;

calcul d'une signature numérique d'une concaténation des signatures numériques obtenues des nœuds non-feuilles correspondant au niveau de nœuds pénultièmes de l'arbre de test, pour ainsi obtenir une signature numérique racine candidate du nœud racine de l'arbre de test ; et

fait de contrôler si la signature numérique racine candidate obtenue coïncide avec la signature numérique racine de référence stockée,

moyennant quoi, dans le cas où lesdites signatures numériques racines coïncident, les données d'article sur l'objet de test ou l'image numérique d'article sont celles d'un article authentique.

10. Procédé selon revendication 9, dans lequel l'article d'origine marqué est sécurisé selon le procédé selon la revendication 8, 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 sur l'objet de test comprend le calcul avec la fonction unidirectionnelle d'une signature numérique d'une concaténation des données

numériques d'article de test extraites et des données numériques du bloc de données de champs stocké.

11. Procédé selon l'une quelconque des revendications 9 et 10, dans lequel l'article est sécurisé par stockage de la signature numérique racine de référence dans une base de données racine consultable accessible à l'utilisateur selon le procédé selon la revendication 2, et l'imageur est en outre équipé d'une unité de communication servant à envoyer et recevoir en retour des données par l'intermédiaire d'une liaison de communication, comprenant les étapes préliminaires de :

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

stockage de la signature numérique racine reçue dans la mémoire de l'imageur.

12. Procédé selon l'une quelconque des revendications 9 à 11, dans lequel l'article est sécurisé selon le procédé selon la revendication 7 et l'imageur est en outre équipé d'un capteur servant à détecter une caractéristique physique unique respectivement d'un article d'origine marqué, ou d'un objet ou 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 à partir 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'article d'origine marqué, ou de l'objet ou individu associé, comprenant les étapes supplémentaires

de, lors de la visualisation d'un sujet étant ledit article ou ledit objet ou individu associé :

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

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, à l'intérieur d'un critère de tolérance donné, le sujet est considéré comme correspondant respectivement à un article authentique, ou à un objet ou individu associé de manière valide à un article authentique.

13. Article appartenant à un lot d'une pluralité d'articles d'origine et sécurisé contre la contrefaçon ou l'altération selon le procédé selon l'une quelconque des revendications 1 à 8, chaque article d'origine du lot ayant des propres données numériques d'article et une clé de vérification correspondante, ledit lot ayant une signature numérique racine de référence correspondante, l'article comprenant :

un marquage de sécurité lisible par machine appliqué sur l'article et incluant une représentation de ses données numériques d'article et sa clé de vérification.

14. Système pour vérifier l'authenticité d'un article, ou la conformité d'une copie d'un tel article, ou la conformité d'une image numérique d'article d'un tel article, par rapport à un article d'origine marqué appartenant à un lot d'articles d'origine sécurisés selon le procédé selon l'une quelconque des revendications 1 à 7, comprenant un imageur ayant une

unité d'imagerie, une unité de traitement comportant une mémoire, et une unité de traitement d'image, la mémoire stockant une signature numérique racine de référence d'un arbre correspondant au lot d'articles d'origine, et la fonction unidirectionnelle pour calculer une signature numérique de données numériques et d'une concaténation de signatures numériques selon l'ordonnancement des nœuds dans l'arbre et l'ordonnancement de concaténation d'arbre étant programmée dans l'unité de traitement, ledit système servant à :

acquérir avec l'imageur une image numérique d'un marquage de sécurité sur un objet de test étant ledit article ou ladite copie de l'article, ou obtenir par l'imageur ladite image numérique d'article montrant un marquage de sécurité sur l'article ;

lire avec l'imageur une représentation de données numériques d'article et d'une clé de vérification associée sur l'image numérique acquise du marquage de sécurité sur l'objet de test, et extraire respectivement des données numériques d'article de test correspondantes et une clé de vérification de test à partir de ladite représentation lue ;

vérifier si les données numériques d'article de test extraites et la clé de vérification associée correspondent bien à la signature numérique racine de référence stockée en exécutant sur l'unité de traitement les étapes programmées supplémentaires de :

calcul avec la fonction unidirectionnelle d'une signature numérique de test à partir de la signature numérique calculée des données numériques d'article 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 sur l'objet de test ;

extraction à partir de la séquence de signatures numériques dans la clé de vérification 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 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, pour ainsi obtenir une signature numérique dudit même nœud parent du nœud feuille de test ;

successivement à chaque niveau suivant dans l'arbre de test et jusqu'au niveau de nœuds pénultièmes, extraction à partir de la séquence de signatures numériques dans la clé de vérification 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 antérieur considéré à l'étape précédente et 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 antérieur, pour ainsi obtenir une signature numérique dudit même nœud parent dudit même nœud parent antérieur ;

calcul d'une signature numérique d'une concaténation des signatures numériques obtenues des nœuds non-feuilles correspondant au niveau de nœuds pénultièmes de l'arbre de test, pour ainsi obtenir une signature numérique racine candidate du nœud racine de l'arbre de test ; et

fait de contrôler si la signature numérique racine candidate obtenue coïncide avec la signature numérique racine de référence stockée,

moyennant quoi, dans le cas où lesdites signatures numériques racines coïncident, le système est configuré

pour délivrer une indication que les données d'article sur l'objet de test ou l'image numérique d'article sont celles d'un article authentique.

15. Système selon revendication 14, dans lequel l'article d'origine marqué est sécurisé selon le procédé selon la revendication 8, 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 sur l'objet de test comprend le calcul avec la fonction unidirectionnelle d'une signature numérique d'une concaténation des données numériques d'article de test extraites et des données numériques du bloc de données de champs stocké.