(19) RÉPUBLIQUE FRANÇAISE

INSTITUT NATIONAL
DE LA PROPRIÉTÉ INDUSTRIELLE

COURBEVOIE

(11) **N° de publication :** **3 082 644**
(à n'utiliser que pour les commandes de reproduction)

(21) **N° d'enregistrement national :** **18 72985**

(51) Int Cl[8] : ***G 06 K 9/00*** *(2019.01), G 06 F 21/60, G 09 F 9/00*

(12) **BREVET D'INVENTION** **B1**

# (54) PROCEDE POUR VERIFIER L'AFFICHAGE D'UN CONTENU PAR UN DISPOSITIF D'AFFICHAGE NUMERIQUE ET SYSTEME D'AFFICHAGE NUMERIQUE.

(22) **Date de dépôt :** 14.12.18.

(30) **Priorité :**

(43) **Date de mise à la disposition du public de la demande :** 20.12.19 Bulletin 19/51.

(45) **Date de la mise à disposition du public du brevet d'invention :** 26.06.20 Bulletin 20/26.

(56) **Liste des documents cités dans le rapport de recherche :**

*Se reporter à la fin du présent fascicule*

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

◯ **Demande(s) d'extension :**

(71) **Demandeur(s) :** *JCDecaux SA Société anonyme* — FR.

(72) **Inventeur(s) :** BASU Anirvan.

(73) **Titulaire(s) :** JCDecaux SA Société anonyme.

(74) **Mandataire(s) :** PLASSERAUD IP.

FR 3 082 644 - B1

# Description

## Titre de l'invention : PROCEDE POUR VERIFIER L'AFFICHAGE D'UN CONTENU PAR UN DISPOSITIF D'AFFICHAGE NUMERIQUE ET SYSTEME D'AFFICHAGE NUMERIQUE.

### Domaine technique

[0001] La présente description concerne les procédés pour vérifier l'affichage d'un contenu par un dispositif d'affichage numérique et les systèmes d'affichage numérique.

### Technique antérieure

[0002] Le document WO03052734 décrit un procédé de transmission d'un message codé par un dispositif d'affichage numérique, pour vérifier le contenu affiché par le dispositif d'affichage. Le message est représentatif du contenu affiché.

### Objets

[0003] La présente description a notamment pour but de proposer un procédé pour vérifier l'affichage d'un contenu par un dispositif d'affichage numérique, qui fournisse une preuve solide que le contenu a effectivement été affiché.

[0004] A cet effet, la présente description propose un procédé pour vérifier l'affichage d'un contenu par au moins un dispositif d'affichage numérique,

ledit dispositif d'affichage numérique comprenant une unité centrale, un écran numérique commandé par l'unité centrale et au moins un capteur optique adapté pour détecter un signal lumineux émis par au moins une partie de l'écran numérique,

le procédé comprenant au moins les étapes suivantes:

(a) faire afficher le contenu sur l'écran numérique par ladite unité centrale,

(b) capter, avec ledit au moins un capteur optique, un signal lumineux émis par au moins une partie dudit écran numérique pendant au moins un créneau temporel pré-déterminé pendant que ledit contenu est affiché par ledit écran numérique,

(c) calculer automatiquement, avec un processeur local voisin de l'écran numérique, au moins une première signature (fonction de chiffrage) du signal lumineux capté par ledit au moins un capteur optique pendant ledit au moins un créneau temporel pré-déterminé,

(d) transmettre à au moins un serveur distant, des données d'authentification de contenu fonction de ladite au moins une première signature avec un horodatage,

(e) comparer au moins une signature d'authentification de contenu, fonction des données d'authentification de contenu, avec au moins une signature de référence de contenu qui est calculée de la même façon que la signature d'authentification de

contenu mais à partir d'un contenu planifié prévu pour être affiché sur ledit écran numérique pendant ledit au moins un créneau temporel prédéterminé,
(f) et, si ladite signature d'authentification de contenu correspond à la signature de référence de contenu dudit contenu planifié, générer au moins un jeton d'authentification authentifiant le contenu affiché.

[0005] Grâce à ces dispositions, la signature étant calculée automatiquement et au plus près de l'affichage, elle est très difficilement falsifiable, de sorte que le procédé fournit une preuve forte, réalisée à la source et infalsifiable ensuite, de l'affichage effectif du contenu planifié. De plus, la signature représentant un faible volume de donnée, le procédé est peu consommateur en bande passante lors de la transmission des données d'authentification vers le serveur distant.

[0006] Par ailleurs, le procédé ne nécessite pas de modifier le contenu en y ajoutant des parties codées, ni de masquer une partie du contenu par le ou les capteurs optique(s). Le procédé est robuste par rapport aux éventuelles distorsions d'images ou éventuelles introductions de bruit dans les signaux captés.

[0007] Dans divers modes de réalisation du procédé, on peut éventuellement avoir recours en outre à l'une et/ou à l'autre des dispositions suivantes (seules ou dans toutes leurs combinaisons mutuelles):

[0008] - à l'étape (f), ledit jeton d'authentification est intégré dans une chaîne de blocs cryptographiquement sécurisée (dite « blockchain ») - cette chaîne de blocs rend les preuves d'affichage (les jetons d'authentification) infalsifiables et non-duplicables ;

[0009] - à l'étape (d), on transmet lesdites données d'authentification en flux continu (« streaming ») ;

[0010] - ladite au moins une première signature est calculée par une fonction de chiffrage « LSH » (« Locality Sensitive Hashing ») ;

[0011] - les données d'authentification de contenu et la signature d'authentification de contenu correspondent à la première signature ;

[0012] - à l'étape (c), on calcule plusieurs premières signatures pour chaque contenu, les données d'authentification de contenu transmises à l'étape (d) comprennent les premières signatures du contenu, et la signature d'authentification de contenu utilisée à l'étape (e) est une deuxième signature calculée à partir desdites premières signatures du même contenu ;

[0013] - à l'étape (c), on calcule plusieurs premières signatures pour chaque contenu puis on calcule une deuxième signature à partir desdites premières signatures du même contenu, les données d'authentification de contenu comprennent la deuxième signature, et la signature d'authentification de contenu est ladite deuxième signature ;

[0014] - la deuxième signature est calculée à partir des premières signatures du même contenu selon un arbre de chiffrage de Merkle ;

[0015] - le dispositif d'affichage numérique comprend plusieurs capteurs optiques et on commande lesdits capteurs optiques pour capter lesdits signaux optiques de façon synchronisée respectivement par lesdits capteurs optiques à l'étape (b) ;

[0016] - le dispositif d'affichage numérique comprend plusieurs capteurs optiques et :

. au cours de l'étape (a), on capte respectivement avec les capteurs optiques, les signaux lumineux émis par ledit écran numérique pendant ledit au moins un créneau temporel prédéterminé pendant que ledit contenu est affiché par ledit écran numérique,

. au cours de l'étape (c), on calcule les premières signatures respectives des signaux lumineux captés par les capteurs optiques pendant ledit au moins un créneau temporel ;

[0017] - le procédé utilise plusieurs créneaux temporels prédéterminés pour chaque contenu affiché et au cours de l'étape (b), on capte avec ledit au moins un capteur optique, les signaux lumineux émis par ledit écran numérique pendant lesdits créneaux temporels prédéterminés pendant que ledit contenu est affiché par ledit écran numérique, au cours de l'étape (b), on calcule es premières signatures respectives des signaux lumineux captés par ledit au moins un capteur optique pendant ledit au moins un créneau temporel ;

[0018] - les contenus sont regroupés en campagnes et on calcule pour une campagne donnée, une signature d'authentification de campagne à partir des signatures d'authentification de contenu respectives des contenus affectés à ladite campagne, selon un arbre de chiffrage de Merkle ;

[0019] - ladite signature d'authentification de campagne est calculée par une fonction de chiffrage « LSH » (« Locality Sensitive Hashing ») ;

[0020] - les campagnes sont affectées à des clients et on calcule pour un client donné, une signature client à partir des signatures d'authentification de campagne respectives de campagnes affectées audit client, selon un arbre de chiffrage de Merkle ;

[0021] - ladite quatrième signature est calculée par une fonction de chiffrage « LSH » (« Locality Sensitive Hashing ») ;

[0022] - ledit au moins un capteur optique est adapté pour prendre au moins une image du contenu affiché par l'écran numérique et ledit signal capté est ladite au moins une image ;

[0023] - ledit capteur optique est configuré pour prendre une série d'images du contenu affiché par l'écran numérique et ledit signal capté est formé par ladite série d'images ;

[0024] - ledit au moins un capteur optique comprend une caméra ;

[0025] - chaque créneau temporel a une durée inférieure à 10s, par exemple comprise entre 5s et 10s, de sorte que chaque signal capté est un instantané (« snapshot ») du signal lumineux ;

[0026] - à l'étape (d) on transmet audit au moins un serveur distant, des données supplémentaires relatives par exemple à une qualité de diffusion dudit écran numérique et /

ou à des conditions extérieures et / ou à des critères d'audience, et au cours de l'étape (e), on calcule le jeton d'authentification avec une valeur dépendant à la fois des données d'authentification et des données supplémentaires ;

[0027] - la valeur du jeton d'authentification est représentative d'une valeur monétaire ;

[0028] - avant le calcul de la première signature, on fait corriger des aberrations et dégradations du signal lumineux par un processeur local voisin de l'écran numérique (le processeur qui calcule la première signature ou un autre processeur local).

[0029] Par ailleurs, la présente description a également pour objet un système d'affichage numérique comportant :

- un dispositif d'affichage numérique comprenant une unité centrale, un écran numérique commandé par l'unité centrale et au moins un capteur optique adapté pour détecter un signal lumineux émis par au moins une partie de l'écran numérique,
- au moins un serveur distant,

ladite unité centrale du dispositif d'affichage numérique étant configurée pour :

(a) faire afficher le contenu sur l'écran numérique,

(b) faire capter par ledit au moins un capteur optique, un signal lumineux émis par au moins une partie dudit écran numérique pendant au moins un créneau temporel prédéterminé pendant que ledit contenu est affiché par ledit écran numérique,

(d) transmettre audit au moins un serveur distant, avec un horodatage, des données d'authentification de contenu fonction d'au moins une première signature, ladite première signature étant calculée automatiquement par un processeur local voisin de l'écran numérique à partir signal lumineux capté par ledit au moins un capteur optique pendant ledit au moins un créneau temporel prédéterminé,

ledit au moins un serveur distant étant configuré pour comparer au moins une signature d'authentification de contenu, fonction des données d'authentification de contenu, avec au moins une signature de référence de contenu qui est calculée de la même façon que la signature d'authentification de contenu mais à partir d'un contenu planifié prévu pour être affiché sur ledit écran numérique pendant ledit au moins un créneau temporel prédéterminé,

et ledit au moins un serveur distant étant configuré pour, si ladite signature d'authentification de contenu correspond à la signature de référence de contenu dudit contenu planifié, générer au moins un jeton d'authentification authentifiant le contenu affiché.

[0030] Dans divers modes de réalisation du système, on peut éventuellement avoir recours en outre à l'une et/ou à l'autre des dispositions suivantes (seules ou dans toutes leurs combinaisons mutuelles):

[0031] - ledit au moins un serveur est configuré pour stocker ledit jeton d'authentification dans une chaîne de blocs cryptographiquement sécurisée (« blockchain ») ;

[0032] - ladite unité centrale est configurée pour transmettre lesdites données d'authentification de contenu en flux continu (« streaming ») ;

[0033] - ladite unité centrale est configurée pour calculer ladite au moins une première signature par une fonction de chiffrage « LSH » (« Locality Sensitive Hashing ») ;

[0034] - le dispositif d'affichage numérique comprend plusieurs capteurs optiques commandés par ladite unité centrale pour capter lesdits signaux optiques de façon synchronisée ;

[0035] - le dispositif d'affichage numérique comprend plusieurs capteurs optiques et ladite unité centrale est adaptée pour :

. faire capter respectivement avec les capteurs optiques, des signaux lumineux émis par ledit écran numérique pendant ledit au moins un créneau temporel prédéterminé pendant que ledit contenu est affiché par ledit écran numérique,

. calculer les premières signatures respectives des signaux lumineux captés par les capteurs optiques pendant ledit au moins un créneau temporel prédéterminé ;

[0036] - le procédé utilise plusieurs créneaux temporels prédéterminés pour chaque contenu affiché et ladite unité centrale est configurée pour :

. faire capter avec ledit au moins un capteur optique, des signaux lumineux émis par ledit écran numérique pendant lesdits créneaux temporels prédéterminés pendant que ledit contenu est affiché par ledit écran numérique,

. calculer les signatures respectives des signaux lumineux captés par ledit au moins un capteur optique pendant ledit au moins un créneau temporel prédéterminé ;

[0037] - ledit au moins un capteur optique est adapté pour prendre au moins une image du contenu affiché par l'écran numérique et ledit signal capté est ladite au moins une image ;

[0038] - ledit capteur optique est configuré pour prendre une série d'images du contenu affiché par l'écran numérique et ledit signal capté est formé par ladite série d'images ;

[0039] - ledit au moins un capteur optique comprend une caméra ;

[0040] - chaque créneau temporel a une durée inférieure à 10s, par exemple comprise entre 5s et 10s, de sorte que chaque signal capté est un instantané (« snapshot ») du signal lumineux ;

[0041] - ladite unité centrale est configurée pour transmettre audit au moins un serveur distant, des données supplémentaires relatives par exemple à une qualité de diffusion dudit écran numérique et / ou à des conditions extérieures et / ou à des critères d'audience, et ledit au moins un serveur est configuré pour calculer le jeton d'authentification avec une valeur dépendant à la fois des données d'authentification et des données supplémentaires ;

[0042] - la valeur du jeton d'authentification est représentative d'une valeur monétaire ;

[0043] - ledit au moins un capteur optique est disposé latéralement par rapport à l'écran

numérique, de façon à ne pas recouvrir le contenu affiché par l'écran numérique ;

[0044] Plus généralement, le système peut être adapté pour mettre en œuvre indépendamment ou en combinaison, chacune des fonctionnalités de procédé décrit précédemment.

## Brève description des dessins

[0045] D'autres caractéristiques et avantages apparaîtront au cours de la description suivante d'une de ses formes de réalisation, donnée à titre d'exemple non limitatif, en regard des dessins joints.

[0046] Sur les dessins :

[0047] [fig.1]

la figure 1 est une vue schématique partielle d'un système d'affichage numérique,

[0048] [fig.2]

la figure 2 est un schéma bloc représentant certains composants d'un dispositif d'affichage numérique du système de la figure 1, et

[0049] [fig.3]

la figure 3 est un diagramme illustrant certaines étapes de traitement des données dans le système de la figure 1.

## Description plus détaillée

[0050] Sur les différentes figures, les mêmes références désignent des éléments identiques ou similaires.

[0051] La figure 1 montre un système d'affichage numérique (numérique) comportant :

- au moins un dispositif d'affichage numérique 1 (généralement, une pluralité de dispositif d'affichage numérique 1),
- au moins un serveur distant 5 (S).

[0052] L'expression « au moins un serveur distant » désigne soit un serveur physique ou virtuel unique, soit plusieurs serveurs physiques ou virtuels appartenant le cas échéant à une informatique en nuage.

[0053] Chaque dispositif d'affichage numérique 1 (DISP DEV) peut comprendre notamment (voir figures 1 et 2) :

- un bâti 2,
- une unité centrale 6 (CU) tel qu'un ordinateur ou similaire, généralement disposée dans le bâti 2,
- un écran numérique 3 (DISP) porté par le bâti 2 et commandé par l'unité centrale 6,
- un ou des capteurs optiques 4 (CAM) tels que notamment des caméras numériques, communiquant avec l'unité centrale 6 et adaptés pour détecter chacun un signal lumineux émis par au moins une partie de l'écran numérique 3,
- éventuellement un ou des capteurs supplémentaires 9, 10 (SENS1, SENS2) com-

muniquant avec l'unité centrale 6.

[0054] Les capteurs supplémentaires 9, 10 peuvent être en nombre quelconque et adaptés notamment pour détecter :

- des conditions externes telles que luminosité, température,
- des caractéristiques de l'audience (notamment nombre de personnes et / ou mouvements de personnes et / ou caractéristiques des personnes tels que notamment âge et sexe, et / ou humeur ou comportement des personnes – dans ce cas le ou les capteurs externes peuvent être choisis notamment parmi les caméras, les détecteurs Wi-Fi ou Bluetooth®, etc.),
- une qualité de diffusion d'images par l'écran numérique 3 (incluant notamment fonctionnement de l'écran numérique 3, définition de l'image, etc.).

[0055] Les capteurs supplémentaires 9, 10 peuvent être en nombre quelconque et peuvent éventuellement communiquer avec l'unité centrale 6 par un réseau radio courte portée, en mode Internet des Objets (IDO). Les capteurs optiques peuvent communiquer avec l'unité centrale 6 par voie filaire, mais pourraient le cas échéant communiquer avec l'unité centrale 6 par un réseau radio courte portée, en mode Internet des Objets (IDO).

[0056] Chaque capteur optique 4 est disposé latéralement par rapport à l'écran numérique 3, de façon à ne pas recouvrir le contenu affiché par l'écran numérique 3. Il prend une image, par exemple partielle, du contenu affiché par l'écran numérique 3, schématisée par les zones 4a respectives des capteurs optiques 4 sur la figure 1.

[0057] L'unité centrale 6 peut comporter au moins un processeur 7 (PROC) et au moins une mémoire 8 (MEM). Dans ce qui suit, les traitements numériques (correction d'image, calcul de première signature, éventuellement calcul de deuxième signature) sont essentiellement réalisés par le processeur 7 de l'unité centrale 6, mais plus généralement certains traitements pourraient être réalisés par tout processeur local voisin de l'écran numérique 3, par exemple des processeurs intégrés aux capteurs 4 et / ou 9, 10.

[0058] L'unité centrale 6 est configurée pour faire afficher des contenus, par exemple des vidéos ou autres, sur l'écran numérique 3. Les contenus peuvent par exemple être affichés par exemple séquentiellement en suivant une liste déterminée (« playlist »). Les contenus et le cas échéant les listes (« playlists ») peuvent être reçus du au moins un serveur 5 ou d'autres serveurs.

[0059] L'unité centrale 6 est configurée pour faire capter par chaque capteur optique 4, un signal lumineux émis par la zone 4a correspondante dudit écran numérique pendant au moins un créneau temporel prédéterminé t1 ou éventuellement pendant plusieurs créneaux temporels t1, t2, etc. pendant que ledit contenu est affiché par ledit écran numérique.

[0060] Avantageusement, lorsqu'il y a plusieurs capteurs optiques 4, l'unité centrale 6 commande les différents capteurs optiques 4 pour capter lesdits signaux optiques de

façon synchronisée. Lorsqu'il y a un ou des capteurs supplémentaires 9, 10, l'unité centrale 6 peut aussi les commander pour capter de façon synchronisée entre eux et / de façon synchronisée avec le ou les capteurs optiques 4.

[0061] Chaque créneau temporel peut avoir une durée inférieure à 10s, par exemple de 5 à 10s. Lorsque le capteur optique 4 est une caméra, le signal lumineux capté est ainsi une courte vidéo (séquence d'images) formant un instantané (c'est-à-dire une capture instantanée ou « snapshot ») du contenu.

[0062] A cette étape (S0 sur la figure 3), l'unité centrale 6, pour chaque contenu (par exemple le contenu CONT 1), stocke des instantanés INST CAM 1, INST CAM 2, etc. pris par les différents capteurs optiques 4 sur le ou les créneaux temporels t1, t2, etc. correspondant à ce contenu.

[0063] Avantageusement, les instantanés peuvent faire l'objet d'un traitement d'image à l'étape S0, pour compenser les distorsions et bruits introduits par le fait que les capteurs optiques 4 sont généralement fortement inclinés par rapport à la surface de l'écran numérique. Ce traitement d'image, connu en soi, peut notamment faire appel à un filtre de Kalman. Le traitement d'image à l'étape S0 peut être réalisé par l'unité centrale 6, ou dans un processeur propre à chaque capteur optique 4, ou dans tout autre processeur local proche de l'écran numérique 3.

[0064] L'unité centrale 6 est configurée pour calculer automatiquement une première signature (étape S1 sur la figure 3) de chaque instantané correspondant à chaque contenu (par exemple pour le contenu CONT 1, une première signature SIGN CAM 1(t1) pour l'instantané provenant du capteur optique CAM 1 au créneau temporel t1, une première signature SIGN CAM 2(t1) pour l'instantané provenant du capteur optique CAM 2 au créneau temporel t1, etc.).

[0065] La première signature peut être une fonction de chiffrage (hachage), notamment de type « LSH » (« Locality Sensitive Hashing »).

[0066] A l'étape S2, l'unité centrale 6 détermine une deuxième signature (SIGN CONT 1) à partir de toutes les premières signatures correspondant à un même contenu. Dans le cas particulier où un ou des écrans numériques 3 seraient équipés d'un seul capteur optique 4 et prendraient un seul instantané (sur un seul créneau temporaire) par contenu, le calcul de la deuxième signature n'a pas lieu d'être et les comparaisons de signatures expliquées ci-dessous seraient faites directement à partir de la première signature de chaque contenu.

[0067] La deuxième signature et les premières signatures forment avantageusement une structure de données hiérarchique en arbre de chiffrage (hachage) de Merkle.

[0068] La deuxième signature peut être une fonction de chiffrage (hachage), notamment de type « LSH » (« Locality Sensitive Hashing »).

[0069] On notera que les premières signatures et / ou la deuxième signature peuvent être

calculées par un processeur autre que le processeur 7 de l'unité centrale 6. Par exemple, chaque première signature pourrait être calculée par un processeur interne à chaque capteur optique 4 ou affecté à chaque capteur optique 4, et la deuxième signature pourrait être calculée par l'unité centrale 6 à partir des premières signatures reçues de ces processeurs.

[0070] A l'étape S2, l'unité centrale 6 transmet audit au moins un serveur distant 5, la deuxième signature (ou plus généralement des données d'authentification de contenu fonction des premières signatures) avec un horodatage. L'unité centrale 6 peut être configurée pour transmettre lesdites données d'authentification de contenu vers ledit au moins un serveur 5 en flux continu (« streaming »). Cette transmission prend la forme d'une série de messages alphanumériques représentant chacun un faible volume de données, ne contenant pas les instantanés eux-mêmes.

[0071] En pratiques, les données d'authentification de contenu peuvent être ou comprendre la deuxième signature de chaque contenu.

[0072] On notera que les données d'authentification de contenu pourraient aussi être transmises audit au moins un serveur 5 à l'étape S1, auquel cas lesdites données d'authentification de contenu sont ou comprennent les premières signatures. Dans ce cas, la deuxième signature peut éventuellement être calculée par le au moins un serveur 5 de la même façon que décrit ci-dessus, ou bien le au moins un serveur 5 ne calcule pas de deuxième signature et utilise directement la ou les premières signature(s) pour authentifier le contenu affiché (par exemple, mais non exclusivement dans le cas susmentionné d'une seule première signature par contenu).

[0073] Dans tous les cas, le serveur dispose d'au moins une signature d'authentification de contenu (première(s) signature(s) ou deuxième signature) de chaque occurrence de contenu, jouée sur chaque écran numérique 3.

[0074] A l'étape S'2, ledit au moins un serveur distant 5 compare ladite au moins une signature d'authentification de chaque occurrence de contenu avec un contenu planifié prévu pour être affiché sur l'écran numérique 3 pendant chaque créneau temporel correspondant à ladite occurrence de contenu jouée sur l'écran numérique 3.

[0075] Plus précisément, le au moins un serveur 5 compare chaque signature d'authentification de contenu avec une signature de référence calculée à partir du contenu planifié. A cet effet, ledit au moins un serveur 5 :

- pour chaque contenu, simule l'enregistrement des instantanés correspondant aux différents capteurs optiques pendant des créneaux temporels correspondant aux créneaux temporels où sont réellement captés les instantanés par les capteurs optiques (autrement dit, les instantanés simulés ainsi obtenus correspondant aux mêmes images du contenu que les instantanés captés par les capteurs optiques, après traitement d'image de ces instantanés captés),

- pour chaque contenu, calcule la ou les signature(s) de référence de la même façon qu'est calculée la ou les signature(s) d'authentification susmentionnée(s) de ce contenu,
- compare chaque signature d'authentification de contenu à la signature de référence du contenu planifié.

[0076] Si cette comparaison indique que la ou les signature(s) d'authentification est / sont identique(s) à la ou les signatures(s) de référence, le au moins un serveur 5 en déduit que le contenu affiché sur l'écran numérique 3 correspond audit contenu planifié, et ledit serveur 5 génère un jeton d'authentification JET CONT 1 immuable authentifiant le contenu affiché (CONT 1 dans cet exemple).

[0077] Ledit au moins un serveur 5 peut être configuré pour stocker ledit jeton JET CONT 1 dans une chaîne de blocs cryptographiquement sécurisée (« blockchain »).

[0078] Les différents contenus sont généralement regroupés en campagnes et ledit au moins un serveur 5 peut être configuré pour calculer pour une campagne donnée (par exemple CAMP 1), une troisième signature, dite signature de campagne, à partir des données d'authentification de contenu correspondant à chaque contenu affecté à ladite campagne, notamment à partir des deuxièmes signatures respectives des contenus affectés à ladite campagne CAMP 1 (étape S3). Ladite troisième signature peut être aussi calculée par une fonction de chiffrage « LSH » (« Locality Sensitive Hashing »). Les premières, deuxièmes et troisièmes signatures peuvent former une structure de données en arbre de chiffrage de Merkle. Par comparaison avec les données dudit au moins un serveur 5 concernant les contenus prévus pour la campagne CAMP 1, ledit au moins un serveur 5 peut déterminer un jeton d'authentification JET CAMP 1 immuable de chaque campagne CAMP 1 (étape S'3). Ledit au moins un serveur 5 peut être configuré pour stocker ledit jeton JET CAMP 1 dans ladite chaîne de blocs cryptographiquement sécurisée (« blockchain »).

[0079] Les campagnes sont affectées à des clients et ledit au moins un serveur 5 peut être configuré pour calculer pour un client donné CLT1, une quatrième signature, dite signature client, à partir des troisièmes signatures respectives de campagnes CAMP 1, CAMP 2, etc. affectées audit client CLT 1 (étape S4). Ladite quatrième signature peut être aussi calculée par une fonction de chiffrage « LSH » (« Locality Sensitive Hashing »). Les premières, deuxièmes, troisièmes et quatrièmes signatures peuvent former une structure de données en arbre de chiffrage de Merkle. Par comparaison avec les données dudit au moins un serveur 5 concernant les contenus prévus pour les campagnes CAMP 1, CAMP 2, etc. du client CLT 1, ledit au moins un serveur 5 peut déterminer un jeton d'authentification JET CLT 1 immuable relatif au client CLT 1 (étape S'4). Ledit au moins un serveur 5 peut être configuré pour stocker ledit jeton JET CLT 1 dans ladite chaîne de blocs cryptographiquement sécurisée

(« blockchain »).

[0080] Les jetons d'authentification permettent ainsi d'authentifier, de façon fiable pour les clients ayant souhaité diffuser leurs contenus sur les dispositifs d'affichage numériques 1, que ces contenus ont été effectivement affichés.

[0081] Par ailleurs, l'unité centrale 6 peut être configurée en outre pour transmettre audit au moins un serveur 5 distant, des données supplémentaires provenant notamment des capteurs supplémentaires 9, 10 susmentionnés et / ou des données externes telles que des données provenant de réseaux sociaux (données pertinentes pour qualifier ou quantifier l'audience ou d'autres conditions externes). Les jetons d'authentification des contenus (JET CONT 1, JET CONT 2, etc.) peuvent alors être calculés par ledit au moins un serveur 5 avec une valeur dépendant à la fois des données d'authentification de contenu (notamment première(s) ou deuxième signature(s)) et desdites données supplémentaires. En particulier, la valeur du jeton d'authentification ou un partie dudit jeton peut être représentative d'une valeur monétaire de chaque diffusion de contenu par un dispositif d'affichage numérique 1, reflétant notamment l'audience touchée et / ou la qualité de diffusion. Cette disposition peut permettre de facturer de façon différenciée chaque diffusion de contenu. Cette facturation peut éventuellement être automatique, les jetons pouvant par exemple être utilisés comme monnaie virtuelle dans la chaîne de blocs susmentionnée.

[0082] Plus généralement, cette disposition peut permettre non seulement d'apporter la preuve qu'un contenu donné a été affiché sur l'écran numérique 3, mais également, le cas échéant, d'apporter la preuve des conditions extérieures au moment de l'affichage et / ou de l'audience présente au moment de l'affichage.

# Revendications

[Revendication 1] Procédé pour vérifier l'affichage d'un contenu par au moins un dispositif d'affichage numérique (1),
ledit dispositif d'affichage numérique (1) comprenant une unité centrale (6), un écran numérique (3) commandé par l'unité centrale (6) et au moins un capteur optique (4) adapté pour détecter un signal lumineux émis par au moins une partie de l'écran numérique (3),
le procédé comprenant au moins les étapes suivantes :
(a) faire afficher le contenu sur l'écran numérique (3) par ladite unité centrale (6),
(b) capter, avec ledit au moins un capteur optique (4), un signal lumineux émis par au moins une partie dudit écran numérique (3) pendant au moins un créneau temporel prédéterminé pendant que ledit contenu est affiché par ledit écran numérique (3),
(c) calculer automatiquement, avec un processeur local (7) voisin de l'écran numérique (3), au moins une première signature du signal lumineux capté par ledit au moins un capteur optique (4) pendant ledit au moins un créneau temporel prédéterminé,
(d) transmettre à au moins un serveur (5) distant, des données d'authentification de contenu fonction de ladite au moins une première signature, avec un horodatage,
(e) comparer au moins une signature d'authentification de contenu, fonction des données d'authentification de contenu, avec au moins une signature de référence de contenu qui est calculée de la même façon que la signature d'authentification de contenu mais à partir d'un contenu planifié prévu pour être affiché sur ledit écran numérique (3) pendant ledit au moins un créneau temporel prédéterminé,
(f) si ladite signature d'authentification de contenu correspond à la signature de référence de contenu dudit contenu planifié, générer au moins un jeton d'authentification authentifiant le contenu affiché.

[Revendication 2] Procédé selon la revendication 1, dans lequel, à l'étape (f), ledit jeton d'authentification est intégré dans une chaîne de blocs cryptographiquement sécurisée.

[Revendication 3] Procédé selon la revendication 1 ou la revendication 2, dans lequel à l'étape (d), on transmet lesdites données d'authentification en flux continu.

[Revendication 4] Procédé selon l'une quelconque des revendications précédentes, dans

lequel ladite au moins une première signature est calculée par une fonction de chiffrage « LSH ».

[Revendication 5] Procédé selon l'une quelconque des revendications précédentes, dans lequel les données d'authentification de contenu et la signature d'authentification de contenu correspondent à la première signature.

[Revendication 6] Procédé selon l'une quelconque des revendications 1 à 4, dans lequel :
- à l'étape (c), on calcule plusieurs premières signatures pour chaque contenu,
- les données d'authentification de contenu transmises à l'étape (d) comprennent les premières signatures du contenu,
- et la signature d'authentification de contenu utilisée à l'étape (e) est une deuxième signature calculée à partir desdites premières signatures du même contenu.

[Revendication 7] Procédé selon l'une quelconque des revendications 1 à 4, dans lequel :
- à l'étape (c), on calcule plusieurs premières signatures pour chaque contenu puis on calcule une deuxième signature à partir desdites premières signatures du même contenu,
- les données d'authentification de contenu comprennent la deuxième signature,
- et la signature d'authentification de contenu est ladite deuxième signature.

[Revendication 8] Procédé selon la revendication 6 à la revendication 7, dans lequel la deuxième signature est calculée à partir des premières signatures du même contenu selon un arbre de chiffrage de Merkle.

[Revendication 9] Procédé selon l'une quelconque des revendications précédentes dans lequel le dispositif d'affichage numérique (1) comprend plusieurs capteurs optiques (4) et on commande lesdits capteurs optiques (4) pour capter lesdits signaux optiques de façon synchronisée respectivement par lesdits capteurs optiques (4) à l'étape (b).

[Revendication 10] Procédé selon l'une quelconque des revendications précédentes, dans lequel le dispositif d'affichage numérique comprend plusieurs capteurs optiques (4) et :
- au cours de l'étape (a), on capte respectivement avec les capteurs optiques (4), les signaux lumineux émis par ledit écran numérique (3) pendant ledit au moins un créneau temporel prédéterminé pendant que ledit contenu est affiché par ledit écran numérique (3),
- au cours de l'étape (c), on calcule les premières signatures respectives des signaux lumineux captés par les capteurs optiques (4) pendant ledit

au moins un créneau temporel prédéterminé.

[Revendication 11] Procédé selon l'une quelconque des revendications précédentes, dans lequel on utilise plusieurs créneaux temporels prédéterminés pour chaque contenu affiché et :
- au cours de l'étape (b), on capte avec ledit au moins un capteur optique (4), les signaux lumineux émis par ledit écran numérique (3) pendant lesdits créneaux temporels prédéterminés pendant que ledit contenu est affiché par ledit écran numérique,
- au cours de l'étape (c), on calcule les premières signatures respectives des signaux lumineux captés par ledit au moins un capteur optique pendant ledit au moins un créneau temporel prédéterminé.

[Revendication 12] Procédé selon la revendication 8, dans lequel les contenus sont regroupés en campagnes et on calcule pour une campagne donnée, une signature d'authentification de campagne à partir des signatures d'authentification de contenu respectives des contenus affectés à ladite campagne, selon un arbre de chiffrage de Merkle.

[Revendication 13] Procédé selon la revendication 12, dans lequel les campagnes sont affectées à des clients et on calcule pour un client donné, une signature client à partir des signatures d'authentification de campagne respectives de campagnes affectées audit client, selon un arbre de chiffrage de Merkle.

[Revendication 14] Procédé selon l'une quelconque des revendications précédentes, dans lequel ledit au moins un capteur optique (4) est adapté pour prendre au moins une image du contenu affiché par l'écran numérique (3) et ledit signal capté est ladite au moins une image.

[Revendication 15] Procédé selon l'une quelconque des revendications précédentes, dans lequel chaque créneau temporel a une durée inférieure à 10s, notamment comprise entre 5s et 10s.

[Revendication 16] Procédé selon l'une quelconque des revendications précédentes, dans lequel à l'étape (d), on transmet audit au moins un serveur (5) distant des données supplémentaires et au cours de l'étape (e), on calcule le jeton d'authentification avec une valeur dépendant à la fois des données d'authentification et des données supplémentaires.

[Revendication 17] Procédé selon l'une quelconque des revendications précédentes, dans lequel avant le calcul de la première signature, on fait corriger des aberrations et dégradations du signal lumineux par un processeur local (7) voisin de l'écran numérique (3).

[Revendication 18] Système d'affichage numérique comportant :

- un dispositif d'affichage numérique (1) comprenant une unité centrale (6), un écran numérique (3) commandé par l'unité centrale (6) et au moins un capteur optique (4) adapté pour détecter un signal lumineux émis par au moins une partie de l'écran numérique (3),
- au moins un serveur (5) distant,
ladite unité centrale (6) du dispositif d'affichage numérique étant configurée pour :
(a) faire afficher le contenu sur l'écran numérique (3),
(b) faire capter par ledit au moins un capteur optique, un signal lumineux émis par au moins une partie dudit écran numérique pendant au moins un créneau temporel prédéterminé pendant que ledit contenu est affiché par ledit écran numérique,
(d) transmettre audit au moins un serveur distant (5), avec un horodatage, des données d'authentification de contenu fonction d'au moins une première signature, ladite première signature étant calculée automatiquement par un processeur local (7) voisin de l'écran numérique (3) à partir signal lumineux capté par ledit au moins un capteur optique pendant ledit au moins un créneau temporel prédéterminé,
ledit au moins un serveur distant (5) étant configuré pour comparer au moins une signature d'authentification de contenu, fonction des données d'authentification de contenu, avec au moins une signature de référence de contenu qui est calculée de la même façon que la signature d'authentification de contenu mais à partir d'un contenu planifié prévu pour être affiché sur ledit écran numérique (3) pendant ledit au moins un créneau temporel prédéterminé
et ledit au moins un serveur distant (5) étant configuré pour, si ladite signature d'authentification de contenu correspond à la signature de référence de contenu dudit contenu planifié, générer au moins un jeton d'authentification authentifiant le contenu affiché.

[Revendication 19] Système selon la revendication 18, dans lequel ledit au moins un capteur optique (4) est disposé latéralement par rapport à l'écran numérique (3), de façon à ne pas recouvrir le contenu affiché par l'écran numérique (3).

[Fig. 1]

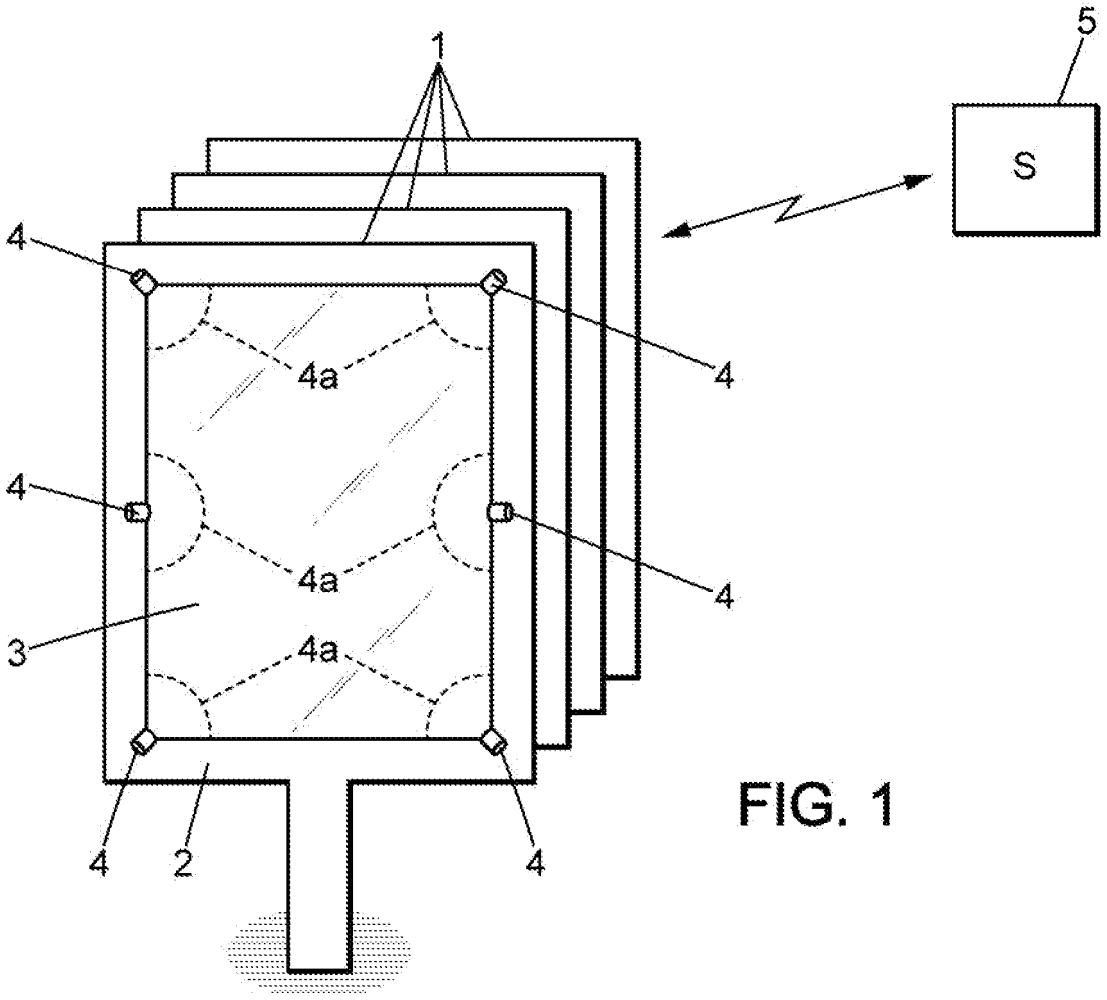


FIG. 1

[Fig. 2]

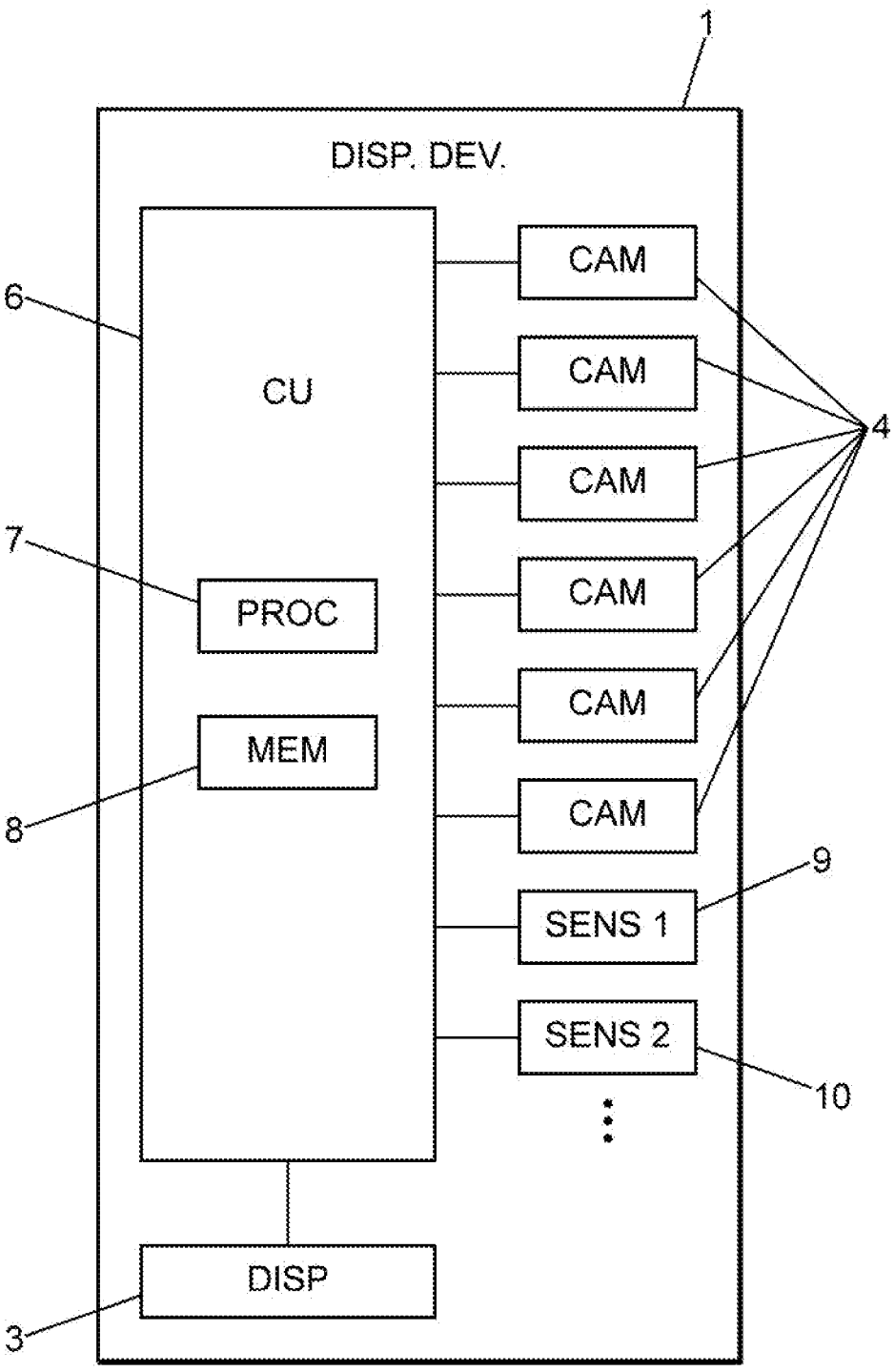
1
DISP. DEV.
6
CU
7
PROC
MEM
8
CAM
CAM
CAM
CAM
CAM
CAM
4
9
SENS 1
SENS 2
10
DISP
3

FIG. 2

[Fig. 3]

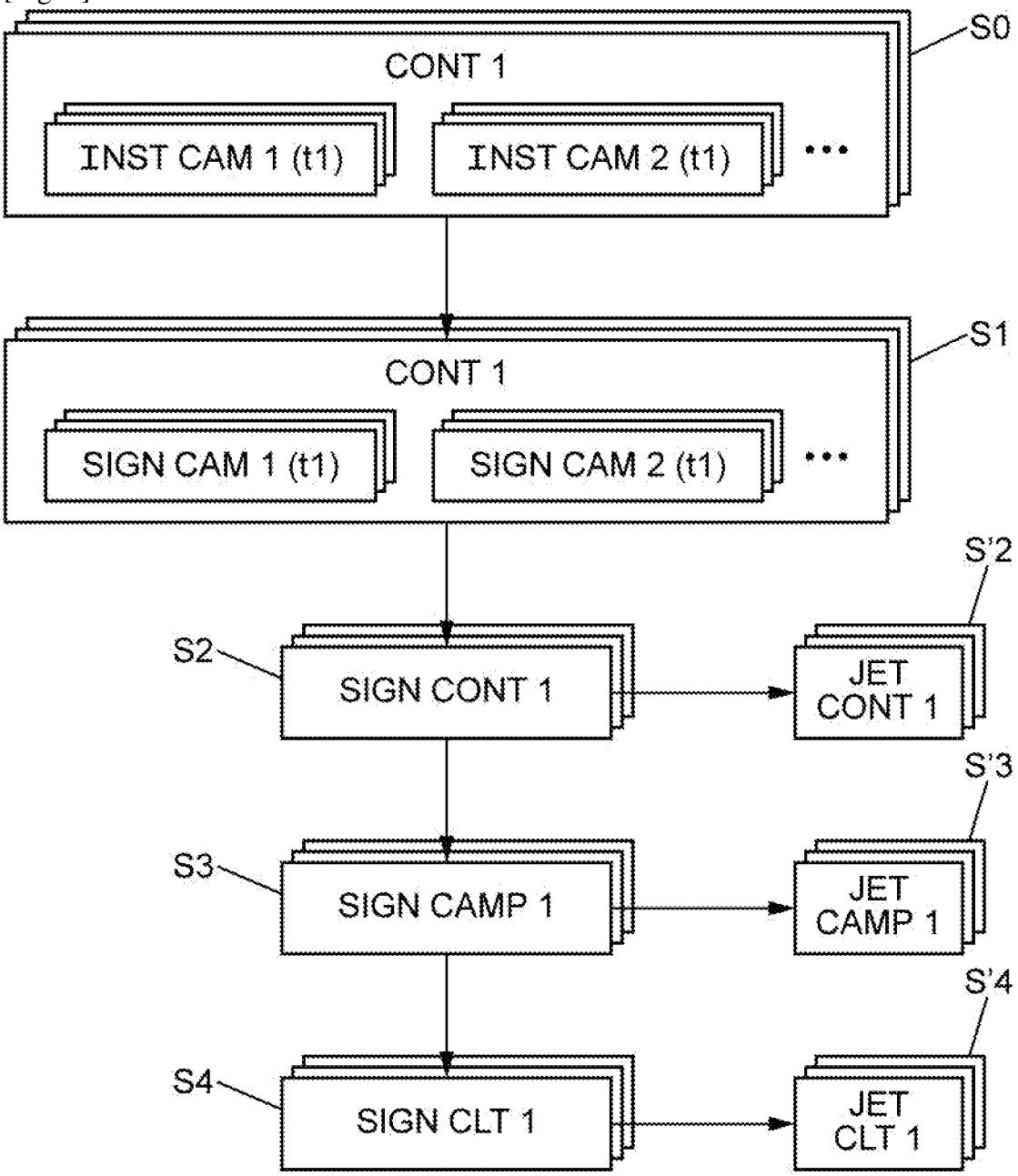
S0
CONT 1
INST CAM 1 (t1)
INST CAM 2 (t1)
S1
CONT 1
SIGN CAM 1 (t1)
SIGN CAM 2 (t1)
S'2
S2
SIGN CONT 1
JET CONT 1
S'3
S3
SIGN CAMP 1
JET CAMP 1
S'4
S4
SIGN CLT 1
JET CLT 1

FIG. 3

# RAPPORT DE RECHERCHE

articles L.612-14, L.612-53 à 69 du code de la propriété intellectuelle

## OBJET DU RAPPORT DE RECHERCHE

L'I.N.P.I. annexe à chaque brevet un "RAPPORT DE RECHERCHE" citant les éléments de l'état de la technique qui peuvent être pris en considération pour apprécier la brevetabilité de l'invention, au sens des articles L. 611-11 (nouveauté) et L. 611-14 (activité inventive) du code de la propriété intellectuelle. Ce rapport porte sur les revendications du brevet qui définissent l'objet de l'invention et délimitent l'étendue de la protection.
Après délivrance, l'I.N.P.I. peut, à la requête de toute personne intéressée, formuler un "AVIS DOCUMENTAIRE" sur la base des documents cités dans ce rapport de recherche et de tout autre document que le requérant souhaite voir prendre en considération.

## CONDITIONS D'ETABLISSEMENT DU PRESENT RAPPORT DE RECHERCHE

[x] Le demandeur a présenté des observations en réponse au rapport de recherche préliminaire.

[x] Le demandeur a maintenu les revendications.

☐ Le demandeur a modifié les revendications.

☐ Le demandeur a modifié la description pour en éliminer les éléments qui n'étaient plus en concordance avec les nouvelles revendications.

☐ Les tiers ont présenté des observations après publication du rapport de recherche préliminaire.

☐ Un rapport de recherche préliminaire complémentaire a été établi.

## DOCUMENTS CITES DANS LE PRESENT RAPPORT DE RECHERCHE

La répartition des documents entre les rubriques 1, 2 et 3 tient compte, le cas échéant, des revendications déposées en dernier lieu et/ou des observations présentées.

[x] Les documents énumérés à la rubrique 1 ci-après sont susceptibles d'être pris en considération pour apprécier la brevetabilité de l'invention.

☐ Les documents énumérés à la rubrique 2 ci-après illustrent l'arrière-plan technologique général.

☐ Les documents énumérés à la rubrique 3 ci-après ont été cités en cours de procédure, mais leur pertinence dépend de la validité des priorités revendiquées.

☐ Aucun document n'a été cité en cours de procédure.

## 1. ELEMENTS DE L'ETAT DE LA TECHNIQUE SUSCEPTIBLES D'ETRE PRIS EN CONSIDERATION POUR APPRECIER LA BREVETABILITE DE L'INVENTION

US 2012/004958 A1 (BLOOM JEFFREY A [US] ET AL) 5 janvier 2012 (2012-01-05)

US 2002/190972 A1 (VEN DE VAN ANTONY [HK]) 19 décembre 2002 (2002-12-19)

Takashi Suzuki ET AL: "A System for End-to-End Authentication of Adaptive Multimedia Content" In: "Communications and Multimedia Security", 1 janvier 2005 (2005-01-01), Springer-Verlag, New York, XP055336188, ISBN: 978-0-387-24485-3 vol. 175, pages 237-249, DOI: 10.1007/0-387-24486-7_18,

## 2. ELEMENTS DE L'ETAT DE LA TECHNIQUE ILLUSTRANT L'ARRIERE-PLAN TECHNOLOGIQUE GENERAL

NEANT

## 3. ELEMENTS DE L'ETAT DE LA TECHNIQUE DONT LA PERTINENCE DEPEND DE LA VALIDITE DES PRIORITES

NEANT