

(12) DEMANDE INTERNATIONALE PUBLIÉE EN VERTU DU TRAITÉ DE COOPÉRATION
EN MATIÈRE DE BREVETS (PCT)

(19) Organisation Mondiale de la Propriété
Intellectuelle
Bureau international



(43) Date de la publication internationale
12 septembre 2008 (12.09.2008)

PCT

(10) Numéro de publication internationale
WO 2008/107528 A2

- (51) Classification internationale des brevets : **Non classée**
- (21) Numéro de la demande internationale : PCT/FR2008/000029
- (22) Date de dépôt international : 10 janvier 2008 (10.01.2008)
- (25) Langue de dépôt : français
- (26) Langue de publication : français
- (30) Données relatives à la priorité :
0752624 11 janvier 2007 (11.01.2007) FR
- (71) Déposant (pour tous les États désignés sauf US) : **MEDI-ALIVE** [FR/FR]; 55, boulevard Romain Rolland, F-92120 Montrouge (FR).
- (72) Inventeurs; et
- (75) Inventeurs/Déposants (pour US seulement) : **FOLEA, Octavian** [FR/FR]; 1, rue René Cassin, F-94270 Le Kremlin Bicetre (FR). **DUPUIS, Sébastien** [FR/FR]; 230, rue du Faubourg Saint-Denis, F-75010 Paris (FR).
- (74) Mandataire : **BREDEMA**; 38, avenue de l'Opéra, F-75002 Paris (FR).
- (81) États désignés (sauf indication contraire, pour tout titre de protection nationale disponible) : AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, SV, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.
- (84) États désignés (sauf indication contraire, pour tout titre de protection régionale disponible) : ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), eurasiatique (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), européen (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MT, NL, NO, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).
- Publiée :
— sans rapport de recherche internationale, sera republiée dès réception de ce rapport

(54) Title: METHOD AND SYSTEM FOR THE SECURED DISTRIBUTION OF DIGITAL DATA

(54) Titre : PROCÉDE ET SYSTEME DE DISTRIBUTION SECURISEE DE DONNEES NUMERIQUES

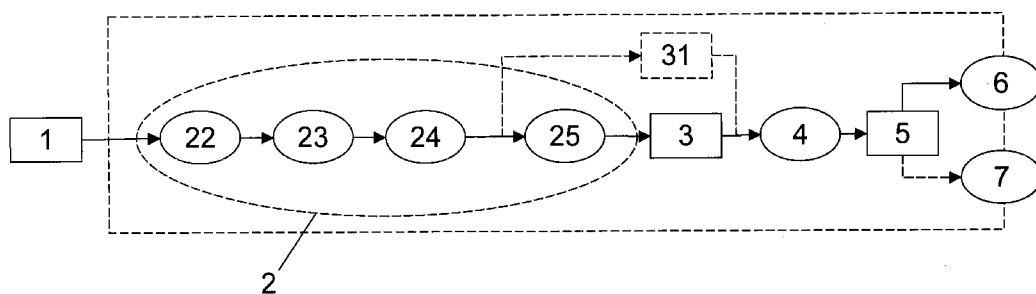


Fig. 2

(57) Abstract: The invention relates to a method for the secured distribution of digital data transmitted to a client terminal (11), said digital data (1) having a first digital format of a non-audiovisual type, wherein said method uses a protection device (4) capable of protecting data (3; 31) having a second digital format and of transmitting said data to said client terminal (11). According to the invention, said second format is of the audiovisual type, and the method comprises a conversion step (2) for converting the digital data (1) having said first digital format into said second format.

(57) Abrégé : L'invention concerne un procédé de distribution sécurisée de données numériques, transmises à un poste client (11), lesdites données numériques (1) se présentant sous un premier format numérique de nature non audiovisuelle, ledit procédé mettant en œuvre un dispositif de protection (4) apte à protéger des données (3; 31) se présentant sous un second format numérique et à les transmettre vers ledit poste client (11). Selon l'invention, ledit second format est de nature audiovisuelle et le procédé comporte une étape de conversion (2) des données numériques (1) se présentant sous ledit premier format dans ledit second format.

WO 2008/107528 A2

PROCEDE ET SYSTEME DE DISTRIBUTION SECURISEE DE DONNEES NUMERIQUES

La présente invention se rapporte au domaine de la protection des
5 données numériques.

La présente invention concerne plus particulièrement un procédé et
un système de distribution sécurisée de données à travers un réseau
de télécommunication ou sur un support physique tel qu'une carte à
10 mémoire ou un DVD.

De manière en soi classique, la présente invention propose un
procédé permettant d'une part de protéger et de distribuer de
manière sécurisée des données numériques jusqu'à un poste
15 utilisateur, les données numériques se présentant sous forme d'une
séquence binaire initiale avant application du procédé, et d'autre
part, de restituer la séquence binaire initiale au niveau du poste
utilisateur, tout en prévenant une utilisation ou un accès non autorisé
aux dites données numériques.

20

On connaît actuellement un développement accru de services
audiovisuels à la demande et à la carte qui sont proposés par des
opérateurs divers, tels que les opérateurs de téléphonie mobile, les
fournisseurs d'accès Internet, les opérateurs de chaînes de télévision
25 par câble et tous les autres fournisseurs de services audiovisuels.

Ces opérateurs déploient massivement des plateformes, c'est-à-dire
des systèmes d'exploitation, du matériel informatique et des
applications logiciels, capables de mettre en oeuvre ces services.

Les plateformes comportent des systèmes appelés systèmes « DRM », (Digital Rights Management) qui contrôlent l'usage qui est fait des œuvres numériques se présentant sous forme de contenus numériques, à travers des réseaux de télécommunication ou sur des supports physiques audiovisuels de type carte à mémoire ou DVD, ce contrôle étant réalisé par la mise en œuvre de procédés de sécurisation ou par tout autre moyen technique apte à autoriser ou interdire la consultation partielle ou totale d'une œuvre numérique.

10

La mise en œuvre de tels systèmes DRM nécessite des développements de moyens techniques et logistiques, désignés ci-après « dispositif(s) de protection ».

15 Pour éviter des utilisations pirates non autorisées des contenus numériques, la plupart des systèmes DRM proposent de transmettre à l'utilisateur un flux audiovisuel numérique protégé, brouillé et généralement crypté par une ou plusieurs clés de codage, de sorte à obtenir un flux audiovisuel de données numériques encodées. Un
20 désembrouillage, ou décodage, du flux chez l'utilisateur est alors conditionné par la réception chez l'utilisateur d'un certificat ou d'une licence qui contient une clé ou plusieurs clés de désembrouillage, le certificat ou la licence étant généralement envoyé à l'utilisateur en échange d'une transaction payante ou non. Le certificat ou la licence
25 contient généralement des éléments de droit liés à de possibles utilisations des contenus numériques désembrouillés.

Les technologies qui sont à la base des systèmes DRM actuels sont diverses et bien connues de l'homme de l'art. Elles se basent sur des spécifications normalisées par des groupes de standardisation, comme OMA DRM 2.0, ISMACryp ou MPEG-21, ou sur des outils
30

logiciels propriétaires, comme Windows Media DRM de Microsoft, Fairplay DRM de Apple et Helix DRM de RealNetworks.

5 Dans la plupart des cas, la protection d'un contenu audiovisuel par un système DRM est conditionnée par :

a) le format d'un conteneur (fichier, flux des données binaires) dans lequel ledit contenu audiovisuel est stocké et transmis ou

b) le type du codeur audiovisuel, si ledit contenu audiovisuel est compressé. Par exemple, Microsoft DRM ne peut protéger que du
10 contenu compressé par un ensemble limité des codeurs, parmi lesquels WMA (Windows Media Audio) ou WMV (Windows Media Vidéo). Dans la même optique, FairPlay DRM ne peut protéger que du contenu audio compressé selon la norme AAC (Advanced Audio codec).

15

Il est connu de l'état de la technique un procédé de distribution sécurisée de données numériques transmises à un poste client, lesdites données numériques se présentant sous un premier format numérique, ledit procédé mettant en œuvre un dispositif de protection apte à protéger des données se présentant sous un
20 second format numérique et à les transmettre vers ledit poste client.

Un tel procédé est le document WO2004/034705A, qui enseigne un procédé et un système pour la distribution sécurisée de données numériques audiovisuelles. Dans ce document, la protection du contenu audiovisuel se fait à deux niveaux. Au
25 premier niveau, des opérations de bruitage sont appliquées sur le contenu présenté sous une forme analogique. Au deuxième niveau, des opérations de cryptage sont appliquées sur le contenu présenté sous une forme digitale et compressée. Le passage entre les deux niveaux comprend une étape de conversion du signal sous une forme analogique dans un signal sous une forme
30 digitale.

Le procédé dévoilé par WO2004/034705A ne peut être appliqué que sur des données audiovisuelles, et pas sur celles de nature autre qu'audiovisuelle. La présente invention se propose donc de résoudre ce problème technique.

5 US2006/095382A1 enseigne un procédé et un système pour la distribution sécurisée de données numériques. Dans ce document, la protection du contenu se fait en utilisant un système DRM (Digital Rights Management) flexible, qui permet de gérer plusieurs systèmes DRM différents.

10 La présente invention propose un procédé alternatif à celui proposé par US2006/095382A1, en utilisant des systèmes DRM déjà déployés et non par proposer un nouveau.

Dans ce procédé, les premier et second formats sont les mêmes. Il
15 s'agit notamment de dispositifs de protection classique qui sécurise la distribution des données numériques audiovisuelles.

Le format du conteneur et le type de codeur empêchent l'usage d'un
20 dispositif de protection à des données dont le format est différent de celui auquel le dispositif est dédié.

Ainsi, à l'heure actuelle, le dispositif de protection de données
numériques audiovisuelles ne protège que des données numériques
audiovisuelles.

25

L'invention a pour objectif d'utiliser les dispositifs de protection de
données numériques audiovisuelles pour protéger des données
numériques autres que celles audiovisuelles.

30 Parallèlement, les services audiovisuels proposés par les fournisseurs présentent des contenus de plus en plus diversifiés :

bien que les séquences numériques les plus sécurisées actuellement par dispositifs de protection sont les séquences audiovisuelles, on assiste à la diversification des données à protéger. Ces dernières peuvent être désormais des documents de textes ou des séquences animées vectorielles (par exemple, des animations respectant le format SWF développé par Macromedia), etc. Ces données de format différent de celui des séquences audiovisuelles seront appelées par la suite « données arbitraires ».

10 Aussi, il est nécessaire de mettre à jour les dispositifs de protection mis en œuvre dans les systèmes DRM pour prendre en compte le format différent des données arbitraires.

Cela entraîne des coûts importants de mise à jour des systèmes DRM, nécessitant de modifier les plateformes au niveau d'un serveur de distribution sécurisée du contenu audiovisuel et au niveau du poste utilisateur.

L'invention a pour objectif de diminuer ces coûts de mise à jour.

20 Au lieu de mettre à jour le dispositif de protection du système DRM lui-même en fonction du format des données arbitraires, l'invention propose un procédé apte à rendre compréhensibles par le système DRM déjà présent sur une plateforme les données arbitraires, sans modifier les dispositifs de protection des systèmes DRM existants.

25

Des autres procédés de protection de la distribution des données audiovisuelles emploient des données complémentaires dans le processus de protection et des reconstituions des données audiovisuelles initiales.

30

L'invention concerne dans un premier temps un procédé de distribution sécurisée de données numériques, transmises à un poste client, les données numériques se présentant sous un premier format numérique de nature non audiovisuelle. Le procédé met en œuvre un
5 dispositif de protection apte à protéger des données se présentant sous un second format numérique et à les transmettre vers le poste client. Selon l'invention, le second format est de nature audiovisuelle et le procédé comporte une étape de conversion des données numériques se présentant sous le premier format numérique dans le
10 second format.

La conversion des données numériques sous un format adapté au dispositif de protection assure de ne pas avoir à modifier le dispositif de protection.

15

Ainsi, l'invention permet de ne pas modifier les systèmes DRM déjà existants et mis en œuvre, et constitue de cette manière un moyen moins coûteux de protéger les données arbitraires se présentant sous un format différent de celui des données audiovisuelles
20 couramment employées par les systèmes DRM.

Suivant une première variante de réalisation, le second format est un format audio de nature audiovisuelle et l'étape de conversion comporte :

- une étape de sélection d'une fréquence et d'une taille
25 d'échantillonnage desdites données numériques identiques respectivement à une fréquence et à une taille correspondant audit second format de données numériques (31),
- une étape d'échantillonnage desdites données numériques en fonction de ladite fréquence et de ladite taille d'échantillonnage
30 sélectionnée selon l'étape de sélection,

- et une étape de création des données numériques sous le second format ayant comme paramètres de définition la fréquence et la taille d'échantillonnage selon l'étape de sélection et comme contenu les échantillons déterminés selon l'étape d'échantillonnage.

On comprend ainsi que le procédé selon l'invention assure la conversion de données numériques se présentant sous n'importe quel format de nature non audiovisuelle, à condition de sélectionner la fréquence et la taille d'échantillon adéquat, de sorte à obtenir des données se présentant sous un format adapté au dispositif de protection.

Suivant une seconde variante de réalisation, l'étape de conversion inclut une étape de codage de données numériques compressées à partir de données numériques non compressées.

Dans le cadre d'une variante de réalisation, l'étape de codage est une étape de codage audio, et elle est réalisée par un dispositif respectant les spécifications Windows Media Audio.

Dans le cadre d'une application particulière du procédé, les données numériques se présentant sous un premier format sont des données d'un second flux de données généré par un dispositif de traitement d'une séquence audiovisuelle nominale comportant des données nominales, le dispositif de traitement générant également un premier flux de données modifiées différentes des données nominales qui est transmis vers le poste client, les données du second flux comprenant des informations numériques complémentaires apte à reconstituer la séquence audiovisuelle nominale.

L'invention vise également un procédé de reconstitution de données numériques dans un premier format numérique de nature non audiovisuelle, à partir de données numériques reçues au niveau d'un poste client en données numériques reconstituées se présentant sous un premier format numérique originel, les données numérique reçues étant protégées. Selon l'invention, le procédé de reconstitution comporte les étapes suivantes :

- 10 - reconstitution des données se présentant sous ledit second format numérique de nature audiovisuelle à partir des données numériques reçues,
- et conversion des données en données numériques reconstituées dans le premier format originel au moyen du dispositif de conversion.

15

Dans le cadre d'une variante de réalisation, l'étape de conversion comporte les étapes suivantes :

- 20 - extraction d'échantillons de données numériques fournies par le dispositif de reconstitution selon une fréquence et une taille d'échantillonnage desdites données numériques,
- et génération d'une séquence de données numériques dans le premier format originel à partir de chaque échantillon extrait selon l'étape d'extraction.

25 Dans le cadre d'une variante de réalisation, l'étape de conversion comporte une étape de décodage de données compressées afin de déterminer des données numériques non compressées pour déterminer la séquence de données numériques sous son format originel.

30

Dans le cadre d'une variante de réalisation, on prévoit que les données numériques de nature non audiovisuelle sont des données d'un second flux de données comprenant des informations numériques complémentaires à celles d'un premier flux de données
5 reçu par le poste client, et que le procédé de reconstitution comporte en outre une étape de reconstitution d'une séquence audiovisuelle nominale en combinant lesdits premier et second flux.

Une fois encore, l'invention permet de maintenir les dispositifs DRM
10 mis en œuvre grâce à l'étape de conversion : les données numériques sont récupérées dans leur format originel grâce à l'étape de conversion.

Bien entendu, ces variantes de réalisation ne sont pas exclusives et
15 le procédé comporter une combinaison de chaque variante précitée ci-dessus.

L'invention vise en outre un système de distribution sécurisée de données numériques à un poste client, les données numériques se
20 présentant sous un premier format numérique de nature non audiovisuelle, le système comportant un dispositif de protection apte à protéger des données se présentant sous un second format numérique, ledit système comportant des moyens de transmission des données protégées audit poste client. Selon l'invention, le
25 second format est de nature audiovisuelle et le système comporte un dispositif de conversion des données numériques se présentant sous le premier format numérique dans le second format numérique.

Dans le cadre d'une variante de réalisation, le dispositif de protection
30 suit les spécifications Windows Media DRM.

Dans le cadre d'une autre variante de réalisation, le système comporte un serveur de licences qui conditionne l'usage des données numériques.

5

Suivant encore une autre variante de réalisation, le système de distribution comprend un dispositif de traitement d'une séquence audiovisuelle nominale comprenant des données nominales, apte à générer un premier flux de données modifiées différentes des données nominales, et un second flux de données complémentaires comprenant des informations numériques complémentaires aptes à reconstituer ladite séquence audiovisuelle nominale en fonction dudit premier flux modifié, lesdites données se présentant sous ledit premier format constituant lesdites données dudit second flux.

15

Enfin, l'invention a pour objet un système de reconstitution de données numériques sous un premier format de nature non audiovisuelle à partir de données numériques reçues, en données numériques reconstituées se présentant sous un premier format numérique originel. Les données numériques reçues sont protégées, et le système comporte un dispositif de reconstitution apte à reconstituer des données numériques sous un second format numérique à partir des données numériques reçues. Selon l'invention, le second format est de nature audiovisuelle et le système comporte un dispositif de conversion apte à convertir les données reconstituées en données numériques dans ledit premier format originel.

Dans le cadre d'une variante de réalisation, le système de reconstitution comporte un dispositif de traitement apte à reconstituer une séquence audiovisuelle nominale comprenant des données

30

nominales, à partir d'un premier flux de données modifiées différentes des données nominales, et d'un second flux de données complémentaires comprenant des informations numériques complémentaires aptes à reconstituer ladite séquence audiovisuelle nominale en fonction dudit premier flux modifié, lesdites données se
5 présentant sous ledit premier format constituant lesdites données dudit second flux.

La présente invention sera mieux comprise à la lecture de la description qui va suivre, en faisant référence à des modes de
10 réalisations illustrés sur les figures annexées, parmi lesquelles :

- la figure 1 représente schématiquement, sous forme de blocs, les étapes principales des procédés selon l'invention à l'émission et à la réception de données,
- 15 - la figure 2 illustre schématiquement, sous forme de blocs, les étapes principales du procédé de distribution selon l'invention,
- la figure 3 montre schématiquement, sous forme de blocs, les étapes principales du procédé de reconstitution de données,
- et la figure 4 présente schématiquement, sous forme de blocs,
20 les étapes principales du procédé de distribution selon l'invention, appliqué à un second flux de données tel que décrit dans la demande WO 2003/065731.

Dans un premier temps, il sera fait plus particulièrement référence
25 à la figure 2 pour décrire un mode de réalisation du procédé de distribution selon l'invention. Dans un second temps, un mode de mise en œuvre du procédé de reconstitution de données sera décrit au regard de la figure 3. Puis, il sera fait référence à la figure 1 pour visualiser la combinaison des procédés de
30 distribution de données au niveau d'un système de diffusion, et de reconstitution de données au niveau d'un poste client. Enfin, on

fera référence à une application particulière du procédé selon l'invention à une séquence audiovisuelle nominale qui est transmise au poste client sous forme d'un premier flux modifié ayant un contenu modifié différent d'un contenu nominal , et d'un
5 deuxième flux complémentaire comprenant des informations numériques complémentaires aptes à reconstituer ladite séquence audiovisuelle nominale en fonction dudit premier flux modifié.

Dans le cadre du mode de réalisation qui sera maintenant exposé, un
10 logiciel DRM est mis en œuvre dans un dispositif de protection 4 suivant les spécifications d'une plateforme WM (Windows Media) DRM.

La plateforme Windows Media DRM est une plateforme de distribution
15 sécurisée de contenus audiovisuels vers des postes utilisateurs 11 à travers des réseaux de télécommunication 6 ou des supports physiques 7 tels que des cartes mémoire ou des DVD.

On cherche à distribuer au poste 11 une œuvre numérique se
20 présentant sous forme de données numériques 1 dans un format qui n'est pas adapté au dispositif de protection 4 de la plateforme Windows Media DRM.

Pour que les données numériques 1 puissent être protégées par le
25 dispositif de protection 4, et conformément à l'invention, les données numériques 1 sont converties dans un format WMA adapté au dispositif de protection 4 au moyen d'un codeur WMA 25 (figure 2).

WMA (Windows Media Audio) est un format propriétaire de compression avec/sans pertes pour les séquences audio de type PCM.

5 La technologie PCM (Pulse Code Modulation pour La Modulation d'Impulsion Codée) est un format numérique pour exprimer des données audio non compressées. Concrètement, pour organiser des données numériques sous le format PCM, on procède de la manière suivante : on représente numériquement un signal analogique en
10 prélevant, à intervalles réguliers, la hauteur du signal. Aussi, pour définir un format PCM, on doit connaître :

- la fréquence d'échantillonnage du signal, cette fréquence étant la cadence de prélèvement du signal. Par exemple, une fréquence de 44,1 kHz représente 44100 échantillons par seconde (ce qui
15 correspond à une qualité audio de disque compact) ;
- la taille de l'échantillon, correspondant à la taille de la représentation numérique de la hauteur de signal pour chaque échantillon. L'unité de mesure est le bit. Par exemple, la qualité de compact disque audio demande un format d'échantillon sur 16
20 bits (ou 2 octets). Une qualité encore meilleure requiert un format d'échantillon sur 24 bits (ou 3 octets).

Le codeur WMA 25 a pour fonction de convertir des données numériques se présentant sous la forme d'une séquence audio 31
25 WAVE en une séquence codée WMA.

Les données audio entrant dans le codeur WMA 25 doivent se présenter sous le format WAVE, un format de type PCM.

Les données numériques se présentant sous un format audio doivent être converties sous le format WMA adapté au dispositif de protection. Pour ce faire, on procède de la manière décrite ci après :

- 5 On met en œuvre un dispositif de conversion 2 comportant un codeur WMA 25, apte à convertir les données numériques 1 en une séquence audiovisuelle 3 codée WMA.

La séquence audiovisuelle 3 est une séquence audio compressée.

10

Suivant une variante de réalisation, le dispositif 2 peut générer une séquence audio non compressée 31 à partir des données numériques 1.

- 15 Suivant cette variante de réalisation, le dispositif de conversion 2 permet de réaliser les étapes suivantes :

Dans une première étape 22, on sélectionne des paramètres de conversion : la fréquence d'échantillonnage (la valeur par défaut est fixée à 44100 Hz) et la taille d'échantillon (la valeur par défaut est fixée à 16 bits).

Dans une seconde étape 23, on découpe des séquences de données numériques 1 au niveau binaire pour les échantillonner suivant la taille choisie selon la première étape.

Puis, dans une troisième étape 24, on génère des données numériques audio non-compressées en format WAVE 31 ayant comme paramètres de définition la fréquence et la taille

d'échantillonnage selon la première étape et comme contenu les échantillons déterminés selon la seconde étape.

Enfin, suivant une ultime étape 25, on met en œuvre le codeur WMA
5 25 pour générer la séquence audio compressée WMA 3 à partir des données numériques audio 31 en format WAVE.

La séquence audio compressée WMA 3, ou la séquence audio non compressée 31, dont les formats respectifs sont adaptés au dispositif
10 de protection 4, sont alors protégées par ce dernier, par des moyens cryptographiques, de sorte à générer des données protégées 5.

A cet effet, le dispositif de protection WM DRM 4 met en oeuvre un outil logiciel appelé WM Rights Manager SDK (Software Development
15 Kit : Outil pour le Développement Logiciel) qui présente deux fonctionnalités principales.

La première fonctionnalité consiste à générer la séquence audio WMA protégée 5 en cryptant la séquence audio compressée WMA 3
20 ou la séquence audio non compressée 31.

La seconde fonctionnalité fait référence à la transmission de licences d'utilisation du contenu au dispositif de reconstitution 41 suite à une tentative de récupération des données numériques audiovisuelles.

25

Dans un autre mode de réalisation, le dispositif de protection WM DRM 4 met en oeuvre un outil logiciel appelé WM Format SDK qui présente deux fonctionnalités principales.

La première fonctionnalité est identique à la première fonctionnalité présentée par WM Rights Manager SDK.

5 La deuxième fonctionnalité consiste à mettre en place un dispositif de reconstitution 41 qui a comme rôle la reconstitution des données numériques audiovisuelles protégées à l'aide de dispositif de protection WM DRM 4.

10 Les données protégées 5 sont alors transmises via le réseau 6 au poste client 11 connecté au réseau.

Suivant une variante de réalisation, on peut également enregistrer sur un support physique 7 les données protégées, suivant une étape 10 représentée par une flèche en traits discontinus sur la figure 2.

15

Dans le cadre de ce mode de réalisation, il convient alors de prévoir, au niveau du poste client, des moyens 71 pour récupérer les données protégées sur le support physique 7.

20 Il sera maintenant fait référence à la figure 3 pour décrire un procédé de reconstitution de données au niveau d'un poste utilisateur.

25 Les données protégées 5 sont reçues par le poste client 11 au niveau d'une entrée 61 reliée au réseau 6, ou bien au niveau des moyens 71 évoqués ci-avant, qui peuvent notamment être constitués par un lecteur de support physique du type lecteur de disque compact ou lecteur carte mémoire.

Les données protégées 5 sont alors transmises à un dispositif de reconstitution 41.

Le dispositif de reconstitution vérifie auprès d'un serveur de licences 5 42 que la licence l'autorise à reconstituer les données. Cette étape est représentée par la flèche à double sens représentée sur la figure 3.

Si la licence autorise la reconstitution des données, le dispositif de 10 reconstitution 41 reconstitue et décode les données de manière en soi connue, de sorte à obtenir des données reconstituées et décodées 31 se présentant sous le format numérique WAVE.

Selon une autre variante de réalisation, le dispositif de reconstitution 15 41 reconstitue les données de manière en soi connue, de sorte à obtenir des données reconstituées 3.

Les données décodées 31 sont alors transmises à un dispositif de 20 conversion 21, qui les convertit en données numériques 1 reconstituées dans le format d'origine.

Selon une autre variante de réalisation, les données reconstituées 3 25 sont alors transmises à un dispositif de conversion 21, qui les convertit en données numériques 1 reconstituées dans le format d'origine.

Pour ce faire, le dispositif de conversion 21 met en œuvre l'étape portant la référence 27 sur la figure 3.

Dans cette dernière étape 27, on génère une séquence de données numériques 1 se présentant sous le format originel, l'étape 27 comportant :

- 5 - une étape d'échantillonnage des données 31 qui sont transmises par le dispositif de reconstitution 41 selon sa fréquence d'échantillonnage et sa taille d'échantillonnage des données 31
- 10 - une étape de génération de l'adite séquence de données numériques 1 en concaténant au niveau binaire chaque échantillon obtenu selon l'étape d'échantillonnage.

Selon une autre variante de réalisation, le dispositif de conversion 21 met en oeuvre une étape supplémentaire 26 avant d'exécuter l'étape 27.

15

Dans l'étape supplémentaire 26, on détermine les données non-compressées 31 en décodant les données numériques compressées 3.

20 La figure 1 illustre la mise en oeuvre des procédés selon l'invention à l'émission et à la réception des données.

25 Le dispositif de conversion 2 convertit les données numériques arbitraires 1 en une séquence audiovisuelle 3 dont le format et éventuellement le codage est adapté au dispositif de protection 4 mettant en oeuvre un logiciel DRM apte à protéger et transformer la séquence audiovisuelle 3 en une séquence audiovisuelle protégée 5.

Selon un autre mode de réalisation, le dispositif de conversion 2 convertit les données numériques arbitraires 1 en une séquence audiovisuelle 31 dont le format et éventuellement est adapté au dispositif de protection 4 mettant en œuvre un logiciel DRM apte à protéger et transformer la séquence audiovisuelle 31 en une séquence audiovisuelle protégée 5.

La séquence audiovisuelle protégée 5, générée par le dispositif de protection 4, est transmise vers le poste client 11 en utilisant deux voies alternatives de transmission: e réseau de télécommunication ou de diffusion classique 6 ou un support physique 7 du type disque compact, DVD, carte mémoire, ou tout autre support physique comportant un mémoire apte à mémoriser des données numériques.

Le poste client 11 récupère ladite séquence audiovisuelle protégée 5 en utilisant le lecteur de supports physiques 71 ou l'interface réseau de télécommunication 61.

Le dispositif de reconstitution 41 récupère la séquence audiovisuelle 31 à partir de la séquence audiovisuelle protégée 5, le dispositif de reconstitution étant compatible avec le dispositif de protection 4.

Selon une autre variante de réalisation, le dispositif de reconstitution 41 récupère la séquence audiovisuelle 3 à partir de la séquence audiovisuelle protégée 5, le dispositif de reconstitution étant compatible avec le dispositif de protection 4.

Le dispositif de reconversion 21 applique l'opération inverse par rapport au dispositif de conversion 2 et il génère ainsi les données numériques arbitraires initiales 1.

On fera maintenant référence à une application particulière du procédé selon l'invention à une séquence audiovisuelle nominale qui est transmise au poste client sous forme d'un premier flux modifié
5 ayant un contenu modifié différent d'un contenu nominal, et d'un deuxième flux complémentaire comprenant des informations numériques complémentaires aptes à reconstituer ladite séquence audiovisuelle nominale en fonction dudit premier flux modifié.

10 Comme il a été indiqué précédemment, un tel procédé est décrit dans la demande de brevet internationale WO 2003/065731.

Cette demande de brevet décrit notamment un procédé pour la distribution sécurisée d'une séquence audiovisuelle à partir d'une
15 séquence audiovisuelle nominale vers un équipement destinataire, ladite séquence audiovisuelle nominale ayant un contenu nominal, le procédé comprenant des étapes dans lesquelles :

- on génère un premier flux modifié ayant un contenu modifié différent du contenu nominal,
- 20 - on génère un deuxième flux complémentaire comprenant des informations numériques complémentaires aptes à reconstituer ladite séquence audiovisuelle originale à partir du calcul en fonction dudit premier flux modifié;
- et on transmet, vers ledit équipement destinataire, ledit premier
25 flux modifié et lesdites informations complémentaires, de sorte à permettre la reconstruction, au niveau de l'équipement destinataire, de ladite séquence audiovisuelle originale.

Le mode de réalisation représenté en figure 4 présente l'avantage de
30 mettre en œuvre un système DRM avec sur un module de

sécurisation connu, par exemple tel que celui décrit dans la demande WO 2003/065731.

Dans le cadre de l'application du procédé à la séquence
5 audiovisuelle sécurisée conformément au procédé décrit dans le
document WO-2003/065731, les données numériques arbitraires
initiales 1 sont constituées par le deuxième flux complémentaire, lui-
même généré par un dispositif de traitement 9 selon le procédé décrit
dans la demande WO 2003/065731. La séquence audiovisuelle
10 originale porte la référence 10 sur la figure 4.

Au moment où le deuxième flux complémentaire est généré, le
dispositif de traitement 9 génère un premier flux nominal modifié 100
pour le distribuer à l'équipement client 11 par l'intermédiaire du
15 réseau 6 ou d'un support physique 7 tel que décrit précédemment.

La consommation de la séquence audiovisuelle originale 10 à partir
un premier flux nominal modifié 100 est conditionnée par la
récupération du deuxième flux complémentaire, donc des données
20 numériques arbitraires initiales 1. La reconstitution des données
numériques arbitraires initiales 1 est réalisée conformément au
procédé selon l'invention.

La séquence audiovisuelle originale 10 est restituée par un dispositif
25 de restitution 91 à partir desdites données numériques arbitraires
initiales 1 et dudit premier flux nominal modifié 100, selon le procédé
décrit par la demande WO 2003/065731.

REVENDICATIONS

1 – Procédé de distribution sécurisée de données numériques, transmises à un poste client (11), ledit procédé mettant en œuvre un
5 dispositif de protection (4) apte à protéger des données (3 ; 31) se présentant sous un second format numérique de nature audiovisuelle et à les transmettre vers ledit poste client (11), le procédé étant caractérisé en ce que ledit premier format est de nature autre qu'audiovisuelle, et en ce que le procédé comporte une étape de
10 conversion (2) des données numériques (1) se présentant sous ledit premier format numérique dans ledit second format.

2 – Procédé de distribution selon la revendication 1, caractérisé en ce que ledit second format est un format audio de nature
15 audiovisuelle et en ce que l'étape de conversion comporte :

- une étape de sélection d'une fréquence et d'une taille d'échantillonnage desdites données numériques identiques respectivement à une fréquence et à une taille correspondant audit second format de données numériques (31),
- 20 - une étape d'échantillonnage desdites données numériques en fonction de ladite fréquence et de ladite taille d'échantillonnage sélectionnée selon l'étape de sélection,
- et une étape de création des données numériques (31) sous le second format ayant comme paramètres de définition la
25 fréquence et la taille d'échantillonnage selon l'étape de sélection et comme contenu les échantillons déterminés selon l'étape d'échantillonnage.

3 – Procédé de distribution selon l'une des revendications
30 précédentes, caractérisé en ce que ladite étape de conversion

comporte une étape de codage de données numériques compressées (3) à partir de données numériques non- compressées (31).

4 – Procédé de distribution selon la revendication 3, caractérisé en ce que l'étape de codage est une étape de codage audio, et en ce qu'elle est réalisée par un dispositif respectant les spécifications Windows Media Audio.

5 – Procédé de distribution selon l'une quelconque des revendications précédentes, caractérisé en ce que lesdites données numériques se présentant sous un premier format sont des données (1) d'un second flux de données généré par un dispositif de traitement (9) d'une séquence audiovisuelle nominale (10) comportant des données nominales, ledit dispositif de traitement (9) générant également un premier flux (100) de données modifiées différentes desdites données nominales qui est transmis vers ledit poste client (11), lesdites données (1) dudit second flux comprenant des informations numériques complémentaires aptes à reconstituer ladite séquence audiovisuelle nominale.

20

6 – Procédé de reconstitution de données numériques (1) dans un premier format numérique de nature autre qu'audiovisuelle à partir de données numériques (5) reçues au niveau d'un poste client en données numériques reconstituées se présentant sous un premier format numérique originel (1), lesdites données numériques reçues étant protégées, caractérisé en ce que le procédé de reconstitution comporte les étapes suivantes :

- reconstitution, au moyen d'un dispositif de reconstitution (41), des données (3 ; 31) se présentant sous ledit second format

30

- numérique de nature audiovisuelle à partir des données numériques (5),
- conversion (21) desdites données (3 ; 31) en données numériques reconstituées (1) dans ledit premier format originel (1) au moyen dudit dispositif de conversion (21).

7 – Procédé de reconstitution selon la revendication 6, caractérisé en ce que ladite étape de conversion (21) comporte les étapes suivantes :

- 10 - extraction d'échantillons de données numériques (31) fournies par le dispositif de reconstitution (41) selon une fréquence et une taille d'échantillonnage desdites données numériques (31),
 - et génération d'une séquence de données numériques (1) dans ledit premier format originel à partir de chaque échantillon
- 15 extrait selon l'étape d'extraction.

8 – Procédé de reconstitution selon la revendication 6 ou 7, caractérisé en ce que ladite étape de conversion comporte une étape de décodage de données compressées (3) afin de déterminer des

20 données numériques non compressées (31).

9- Procédé de reconstitution selon l'une quelconque des revendications 6, 7 ou 8, caractérisé en ce que lesdites données numériques de nature autre qu'audiovisuelle (1) sont des données

25 d'un second flux de données comprenant des informations numériques complémentaires à celles d'un premier flux de données (100) reçu par ledit poste client, ledit procédé comportant une étape de reconstitution d'une séquence audiovisuelle nominale (10) en combinant lesdits premier et second flux.

10 – Système de distribution sécurisée de données numériques à un poste client (11), lesdites données numériques se présentant sous un premier format numérique de nature autre qu'audiovisuelle, ledit système comportant un dispositif de protection (4) apte à protéger
5 des données (3 ; 31) se présentant sous un second format numérique, ledit système comporte des moyens de transmission des données protégées audit poste client, caractérisé en ce que ledit second format est de nature audiovisuelle et en ce ledit système comporte un dispositif de conversion (2) des données numériques se
10 présentant sous ledit premier format numérique dans ledit second format numérique.

11 – Système de distribution selon la revendication 10, caractérisé en ce que ledit dispositif de protection suit les spécifications
15 Windows Media DRM.

12 – Système de distribution selon l'une quelconque des revendications 10 ou 11, caractérisé en ce qu'il comporte un serveur de licences qui conditionne l'usage desdites données numériques.
20

13 – Système de distribution selon l'une quelconque des revendications 10 à 12, caractérisé en ce qu'il comprend un dispositif de traitement (9) d'une séquence audiovisuelle nominale (10) comprenant des données nominales, apte à générer un premier flux
25 de données modifiées (100) différentes des données nominales, et un second flux de données complémentaires (1) comprenant des informations numériques complémentaires aptes à reconstituer ladite séquence audiovisuelle nominale en fonction dudit premier flux modifié, lesdites données se présentant sous ledit premier format
30 constituant lesdites données dudit second flux.

14 – Système de reconstitution de données numériques (1) sous un premier format de nature autre qu'audiovisuelle à partir de données numériques reçues (5), en données numériques reconstituées se présentant sous un premier format numérique originel, lesdites
5 données numériques reçues étant protégées, ledit système comportant un dispositif de reconstitution (41) apte à reconstituer des données numériques (3 ; 31) sous un second format numérique à partir desdites données numériques reçues (5), caractérisé en ce que ledit second format est de nature audiovisuelle et en ce que ledit
10 système comporte un dispositif de conversion (21) apte à convertir lesdites données (3 ; 31) reconstituées en données numériques (1) dans ledit premier format originel.

15 - Système de reconstitution selon la revendication 14, caractérisé
15 en ce qu'il comporte un dispositif de traitement (91) apte à reconstituer une séquence audiovisuelle nominale (10) comprenant des données nominales à partir d'un premier flux de données modifiées (100) différentes des données nominales, et d'un second flux de données complémentaires (1) comprenant des informations
20 numériques complémentaires aptes à reconstituer ladite séquence audiovisuelle nominale en fonction dudit premier flux modifié, lesdites données se présentant sous ledit premier format constituant lesdites données dudit second flux.

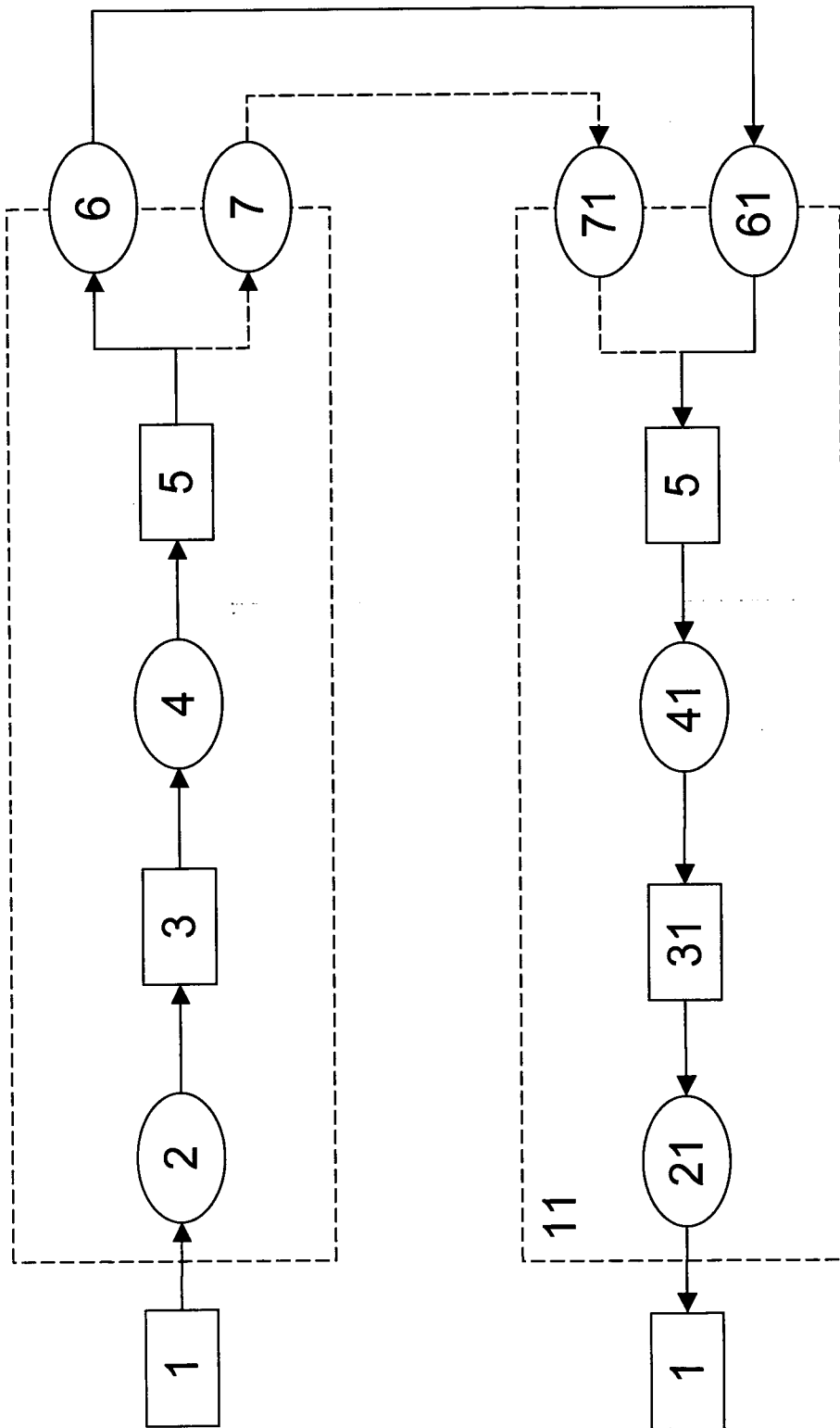


Fig. 1

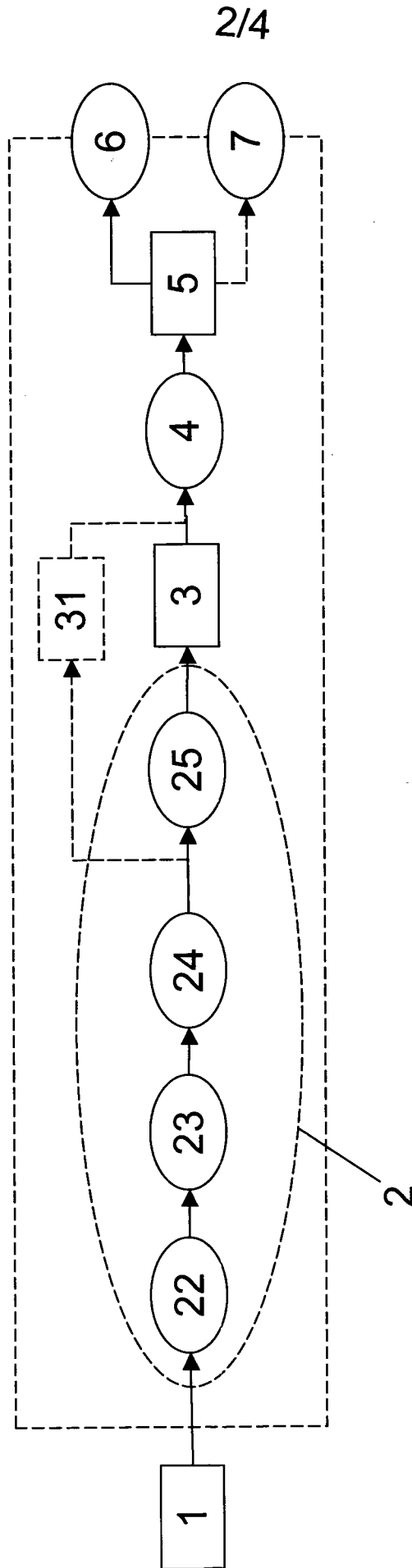


Fig. 2

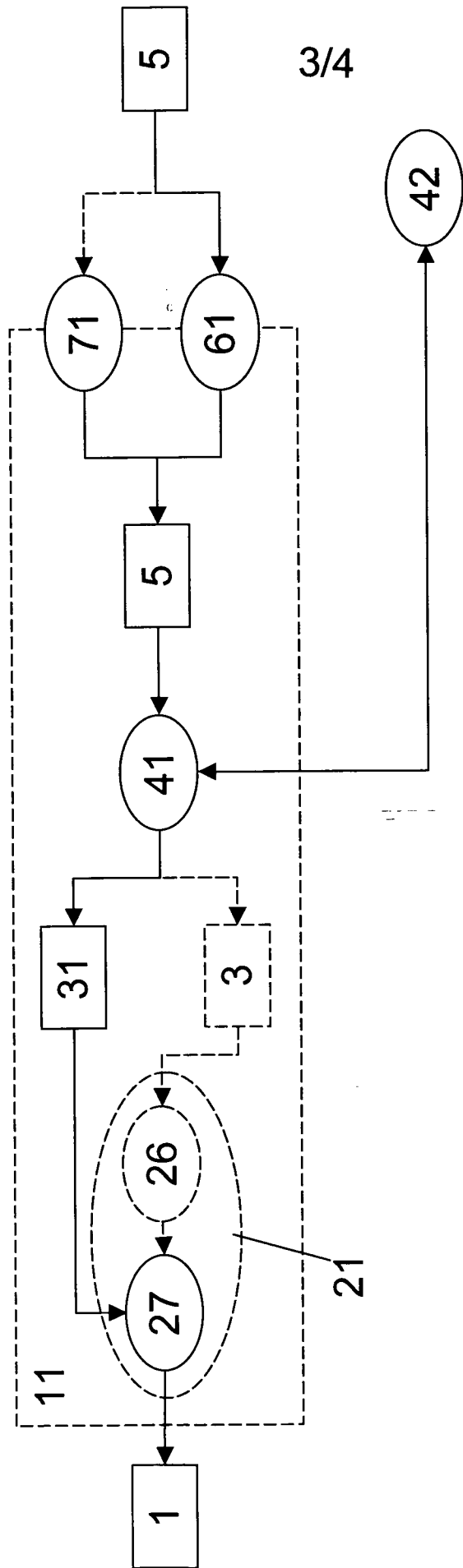


Fig. 3

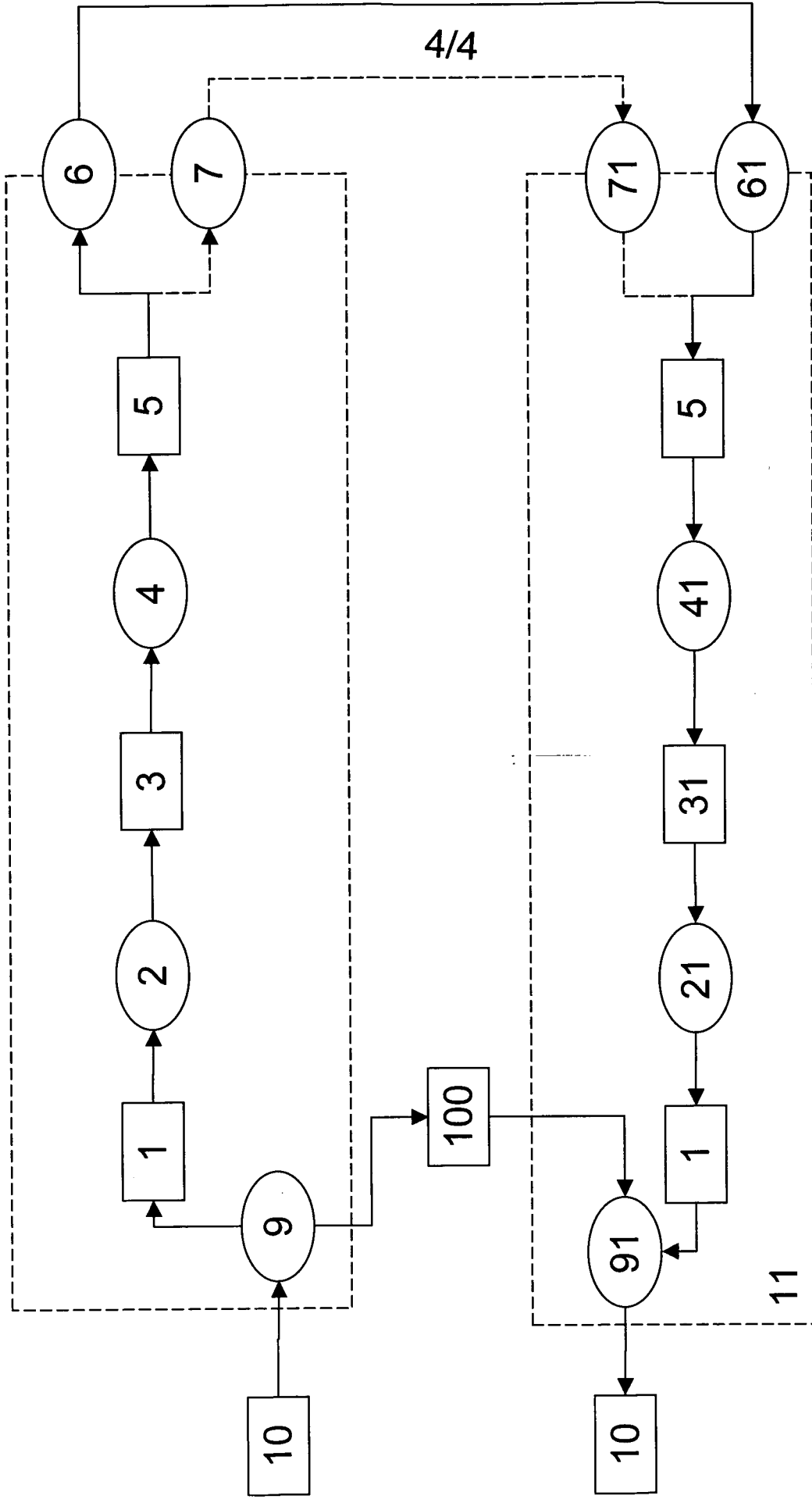


Fig. 4