(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
29 avril 2004 (29.04.2004)

PCT

(10) Numéro de publication internationale
WO 2004/036411 A2

(51) Classification internationale des brevets[7] : G06F 7/00

(21) Numéro de la demande internationale :
PCT/EP2003/050718

(22) Date de dépôt international :
14 octobre 2003 (14.10.2003)

(25) Langue de dépôt : français

(26) Langue de publication : français

(30) Données relatives à la priorité :
0213333 16 octobre 2002 (16.10.2002) FR

(71) Déposant *(pour tous les États désignés sauf US)* : **THOMSON LICENSING S.A.** [FR/FR]; 46 Quai Alphonse Le Gallo, F-92100 BOULOGNE BILLANCOURT (FR).

(72) Inventeur; et

(75) Inventeur/Déposant *(pour US seulement)* : **DIEHL, Eric** [FR/FR]; La Buzardière, F-35340 LIFFRE (FR).

(74) Mandataire : **BERTHIER, Karine**; THOMSON, 46 Quai Alphonse Le Gallo, F-92648 Boulogne cedex (FR).

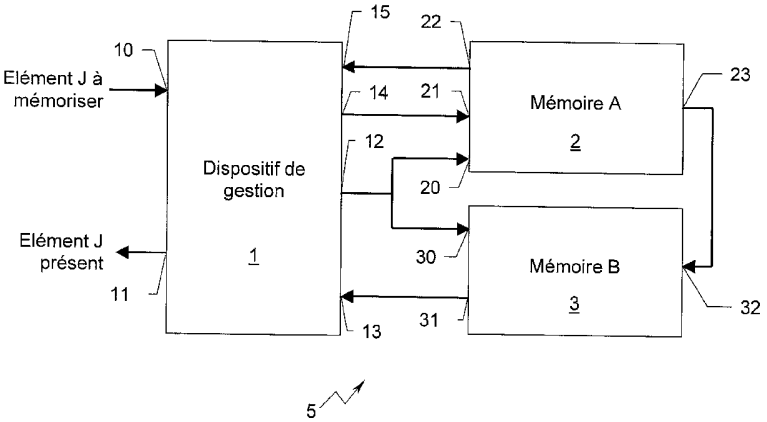
(81) États désignés *(national)* : AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) États désignés *(régional)* : brevet ARIPO (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), brevet eurasien (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), brevet européen (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, RO, SE, SI, SK, TR), brevet OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

[Suite sur la page suivante]

(54) **Title:** DEVICE FOR STORING A LIST OF ELEMENTS AND METHOD OF STORING AN ELEMENT IN ONE SUCH DEVICE

(54) **Titre :** DISPOSITIF DE MEMORISATION D'UNE LISTE D'ELEMENTS ET PROCEDE DE MEMORISATION D'UN ELEMENT DANS UN TEL DISPOSITIF



10 ELEMENT J TO BE STORED
11 ELEMENT J PRESENT
1 MANAGEMENT DEVICE
2 MEMORY UNIT A
3 MEMORY UNIT B

(57) **Abstract:** The invention relates to a device (5) for storing a list of elements, in which any element (J) that has been presented thereto is stored last. The inventive device comprises a first memory unit (3) and means for randomly selecting an element stored in the first memory unit, such that said selected element can be deleted and a new presented element stored when the first memory unit is full and a new element must be stored. The invention also relates to a method of storing an element (J) in one such device (5).

[Suite sur la page suivante]

WO 2004/036411 A2

Publiée :

— *sans rapport de recherche internationale, sera republiée dès réception de ce rapport*

En ce qui concerne les codes à deux lettres et autres abréviations, se référer aux "Notes explicatives relatives aux codes et abréviations" figurant au début de chaque numéro ordinaire de la Gazette du PCT.

(57) Abrégé : L'invention concerne un dispositif (5) de mémorisation d'une liste d'éléments destiné à mémoriser tout élément (J) qui lui a été présenté en dernier lieu. Il comprend une première mémoire (3) et des moyens chargés, lorsque la première mémoire est pleine et qu'un nouvel élément doit être mémorisé, de sélectionner aléatoirement un élément mémorisé dans la première mémoire pour effacer cet élément sélectionné et pour mémoriser le nouvel élément présenté. Elle concerne aussi un procédé de mémorisation d'un élément (J) dans un tel dispositif (5).

Dispositif de mémorisation d'une liste d'éléments et procédé de mémorisation d'un élément dans un tel dispositif

Domaine de l'invention

La présente invention se rapporte d'une manière générale au domaine de la sécurité dans des systèmes qui nécessitent la mémorisation d'un historique sécurisé. Elle concerne plus particulièrement un dispositif de mémorisation d'une liste d'éléments et un procédé de mémorisation d'un élément dans un tel dispositif.

Etat de la technique

Pour se prémunir contre des tentatives illégales d'accès à des données ou des opérations frauduleuses sur des données, il est courant dans les systèmes dits « sécurisés » de conserver un historique d'événements ou une liste d'opérations effectuées.

Un exemple typique concerne un dispositif d'enregistrement qui n'est autorisé à effectuer qu'une copie unique (ou un nombre limité de copies) de chaque contenu qu'il est susceptible d'enregistrer. Ceci est nécessaire avec les dispositifs d'enregistrement numériques pour éviter la prolifération de copies illégales tout en autorisant la copie à usage privé. Une solution immédiate pour garantir ceci consiste à conserver dans le dispositif d'enregistrement une liste de tous les contenus (ou plus précisément une liste d'identifiants de tous les contenus) déjà enregistrés par lui. Chaque fois que le dispositif d'enregistrement reçoit une commande d'enregistrement d'un contenu particulier, il vérifie avant que ce contenu n'est pas présent dans la liste des contenus déjà enregistrés. Si le contenu (ou plus précisément son identifiant) est présent dans la liste, le dispositif d'enregistrement refuse de l'enregistrer.

Le problème qui ressort de l'exemple ci-dessus est que le nombre potentiel de contenus à enregistrer est sans limite. Il faudrait donc pour garantir la sécurité du système que la liste des contenus déjà enregistrés soit aussi sans limite, ce qui n'est pas possible dans les appareils d'électronique grand public. Dans ce type d'appareil, on utilise habituellement une mémoire de type FIFO (acronyme de « First In First Out » signifiant « Premier Entré Premier Sorti ») pour mémoriser une liste telle que ci-dessus.

Mais si le but de cette liste est de garantir une certaine sécurité dans un système, comme dans l'exemple ci-dessus où la liste est tenue pour éviter la copie illicite de contenus, ou bien dans le cas d'une liste de révocation

contenant des identifiants de clés cryptographiques ou d'appareils qui ne sont plus considérés comme conformes ou licites par un organisme de confiance, alors la solution consistant à mémoriser une telle liste dans une mémoire FIFO n'est pas satisfaisante. En effet, si la mémoire a une taille lui permettant de mémoriser n éléments, il suffira à un pirate de présenter n+1 éléments au dispositif mémorisant la liste pour être sûr que le premier élément mémorisé est effacé de la liste, ce qui compromet bien évidemment la sécurité du système.

Exposé de l'invention

La présente invention vise à résoudre les problèmes précités.

Elle a pour objet un dispositif de mémorisation d'une liste d'éléments destiné à mémoriser tout élément qui lui a été présenté en dernier lieu. Ce dispositif comprend une première mémoire et il comporte en outre selon l'invention des moyens chargés, lorsque la première mémoire est pleine et qu'un nouvel élément doit être mémorisé, de sélectionner aléatoirement un élément mémorisé dans la première mémoire pour effacer cet élément sélectionné et pour mémoriser le nouvel élément présenté.

Selon une caractéristique particulière de l'invention, le dispositif est capable de mémoriser N éléments, N étant un entier naturel, et il comporte en outre une deuxième mémoire destinée à mémoriser en permanence les M éléments qui ont été présentés en dernier lieu audit dispositif, M étant un entier naturel inférieur à N, la première mémoire étant destinée à mémoriser les N-M autres éléments.

Grâce au dispositif selon l'invention, même si on lui présente plus de N éléments à mémoriser, il n'y a aucun moyen de savoir à la fin quel(s) élément(s) ne se trouve(nt) plus dans le dispositif.

Selon une autre caractéristique, le dispositif est en outre adapté à fournir une information indiquant si l'élément qui lui a été présenté en dernier lieu est déjà présent dans le dispositif.

Selon encore une autre caractéristique, le dispositif ne contient qu'un seul exemplaire de chaque élément mémorisé.

Selon un aspect particulier de l'invention, le dispositif mémorise en outre, avec chaque élément, le nombre de fois où cet élément lui a été présenté.

Selon un autre aspect de l'invention, le dispositif est adapté à fournir une information indiquant si l'élément qui lui a été présenté en dernier lieu lui a déjà été présenté un nombre de fois qui dépasse un nombre prédéterminé.

L'invention concerne également un procédé de mémorisation d'un élément dans un dispositif tel que décrit ci-dessus. Il comprend les étapes consistant à (a) recevoir un élément qui est présenté au dispositif ; (b) vérifier si cet élément est déjà présent dans le dispositif ; et

- en cas de vérification positive, désigner l'élément comme élément mémorisé en dernier lieu, et
- en cas de vérification négative, mémoriser l'élément dans le dispositif.

Selon un mode de réalisation particulier, en cas de vérification négative à l'étape (b) :

- si la deuxième mémoire n'est pas pleine, l'élément reçu est mémorisé dans la deuxième mémoire ; et
- si la deuxième mémoire est pleine :

i) l'élément le plus ancien mémorisé dans la deuxième mémoire est transféré vers la première mémoire ;

ii) l'élément reçu est mémorisé dans la deuxième mémoire (2) ; et

iii) si la première mémoire est pleine, alors un élément mémorisé dans la première mémoire est sélectionné aléatoirement pour être effacé de sorte que l'élément le plus ancien mémorisé dans la deuxième mémoire puisse être transféré vers la première mémoire.

Brève description des dessins

D'autres caractéristiques et avantages de l'invention apparaîtront à travers la description d'un mode de réalisation particulier non limitatif de celle-ci, explicité à l'aide de la figure unique annexée qui représente de manière schématique un dispositif de mémorisation selon l'invention.

Description détaillée de modes de réalisation de l'invention

Le dispositif de mémorisation de l'invention est prévu pour contenir au maximum N éléments, par exemple des identifiants de contenus à enregistrer. Ce dispositif, qui porte la référence 5 sur la figure unique, est notamment intégré dans un appareil d'enregistrement numérique.

Le dispositif 5 comprend deux mémoires A et B. La mémoire A, référencée 2, contient au maximum M éléments et la mémoire B, référencée 3, contient au maximum P éléments, de sorte que N = M + P, où, N, M et P sont des entiers naturels.

La mémoire A contient toujours les M derniers éléments qui ont été mémorisés dans le dispositif. La mémoire B contient quant à elle des éléments qui ont été mémorisés avant les M derniers éléments.

Lorsqu'un nouvel élément J est présenté au dispositif, par exemple lorsqu'une commande d'enregistrement d'un nouveau contenu est reçue par l'appareil d'enregistrement, l'identifiant du contenu (correspondant à l'élément J) est présenté au dispositif de mémorisation 5 pour vérifier s'il est déjà contenu dans la liste mémorisée dans le dispositif 5 ou non.

Si l'élément J est déjà présent dans la mémoire A, alors il est marqué dans la mémoire A comme dernier élément mémorisé. Si l'élément J est déjà présent dans la mémoire B, alors il est déplacé dans la mémoire A à l'emplacement du dernier élément mémorisé. Dans ces deux cas, le dispositif 5 retourne alors l'information selon laquelle l'élément J est présent.

Si l'élément J n'est présent ni dans la mémoire A ni dans la mémoire B, alors J est mémorisé dans la mémoire A. Si la mémoire A contenait déjà M éléments, alors l'élément le plus ancien mémorisé dans la mémoire A est transmis à la mémoire B pour y être enregistré. Il est en même temps effacé de la mémoire A pour laisser la place à l'élément J. Si la mémoire B est également pleine, c'est à dire si elle contient déjà P éléments, alors un élément déjà mémorisé dans la mémoire B est sélectionné aléatoirement pour être effacé et remplacé par l'élément le plus ancien de la mémoire A. Le dispositif 5 retourne alors l'information selon laquelle l'élément J n'était pas présent mais est maintenant mémorisé.

En se référant plus particulièrement à la figure unique, le dispositif de mémorisation 5 comprend un dispositif de gestion 1 et deux mémoires A et B référencées respectivement 2 et 3.

Le dispositif de gestion 1 possède trois entrées 10, 13 et 15 et trois sorties 11, 12 et 14. L'entrée 10 reçoit l'élément J à mémoriser qui est ensuite transmis à la sortie 12 du dispositif de gestion.

La sortie 11 est un signal booléen qui indique si l'élément J se trouve déjà mémorisé dans le dispositif de mémorisation 5. Le signal présent à la sortie 11 vaut « 1 » (pour « vrai ») si l'élément J est déjà mémorisé et vaut « 0 » (pour « faux ») dans le cas contraire. Les entrées 13 et 15 et la sortie 14 sont également des signaux booléens qui seront décrits ci-dessous.

La mémoire A possède deux entrées 20 et 21 et deux sorties 22 et 23. L'entrée 20 reçoit la sortie 12 du dispositif de gestion qui lui transmet l'élément J à mémoriser ou dont la présence doit être recherchée dans la

mémoire A. L'entrée 21 qui est reliée à la sortie 14 du dispositif de gestion 1 est un signal booléen qui indique, lorsque sa valeur est « 1 » (« vrai ») que l'élément J reçu à l'entrée 20 doit être mémorisé dans la mémoire A.

La sortie 22 de la mémoire A est également un signal booléen qui indique, lorsque sa valeur vaut « 1 » (« vrai »), que l'élément J présenté à l'entrée 20 est déjà présent dans la mémoire A. Cette sortie 22 est reliée à l'entrée 15 du dispositif de gestion 1.

La sortie 23 de la mémoire A est utilisée seulement lorsque la mémoire A est pleine et qu'un nouvel élément présent à l'entrée 20 doit être mémorisé. Dans ce cas, la sortie 23 fournit l'élément le plus ancien mémorisé dans la mémoire A. Dans le cas contraire, la sortie 23 ne fournit aucun signal.

La mémoire B comporte quant à elle deux entrées 30 et 32 et une sortie 31. L'entrée 30 est reliée à la sortie 12 du dispositif de gestion 1 et reçoit l'élément J dont la présence dans la mémoire B doit être vérifiée. La sortie 31 est un signal booléen dont la valeur est « 1 » (« vrai ») lorsque l'élément J reçu à l'entrée 30 est présent dans la mémoire B ; elle est reliée à l'entrée 13 du dispositif de gestion 1.

L'entrée 32 de la mémoire B reçoit quant à elle l'élément à mémoriser qui provient de la mémoire A lorsque cette dernière est pleine. L'entrée 32 est à cet effet reliée à la sortie 23 de la mémoire A.

Le fonctionnement de l'ensemble est le suivant. Lorsque le dispositif de gestion 1 reçoit un élément J sur son entrée 10, il fournit cet élément J à sa sortie 12. Si cet élément J est présent dans la mémoire A, un signal « 1 » (pour « vrai ») est reçu sur l'entrée 15 du dispositif de gestion 1. Si l'élément J est présent dans la mémoire B, un signal « 1 » (pour « vrai ») est reçu à l'entrée 13 du dispositif de gestion 1.

Si les deux signaux booléens reçus sur les entrées 13 et 15 du dispositif de gestion ont une valeur « 0 » (c'est à dire « faux »), cela signifie que l'élément J reçu en entrée 10 n'est présent ni dans la mémoire A ni dans la mémoire B. Dans ce cas, le dispositif de gestion 1 fournit sur sa sortie 11 un signal « 0 » (« faux ») et sur sa sortie 14 un signal « 1 » signifiant que l'élément J doit être enregistré dans la mémoire A.

Si le signal booléen reçu sur l'entrée 15 a une valeur « 1 » (« vrai »), signifiant que l'élément J est déjà présent dans la mémoire A, alors le dispositif de gestion 1 fournit sur sa sortie 11 un signal « 1 » (« vrai ») et sur sa sortie 14 un signal « 0 ».

Dans le cas où le signal booléen reçu sur l'entrée 13 a une valeur « 1 » (« vrai »), signifiant que l'élément J est déjà présent dans la mémoire B, alors le dispositif de gestion 1 fournit sur sa sortie 11 un signal « 1 » (« vrai ») et sur sa sortie 14 un signal « 1 ».

Lorsque la mémoire A reçoit sur son entrée 20 un élément J, elle vérifie tout d'abord si elle contient déjà cet élément. Si l'élément J est déjà présent dans la mémoire A, alors le signal en sortie 22 prend la valeur « 1 » (« vrai »). L'élément J est alors désigné comme l'élément mémorisé en dernier lieu par la mémoire A. Par exemple, l'élément J est placé en tête de pile si la mémoire A a une structure de pile, ou bien une table d'index des éléments stockés dans la mémoire A est mise à jour.

Dans le cas contraire (J non présent dans la mémoire A), la sortie 22 prend la valeur « 0 » (« faux »).

Lorsque le signal reçu sur l'entrée 21 de la mémoire A est « vrai » (valeur « 1 »), signifiant que l'élément J présent sur l'entrée 20 doit être mémorisé dans la mémoire A, il existe deux possibilités. Soit la mémoire A contient moins de M éléments et elle mémorise le nouvel élément J qui devient l'élément mémorisé en dernier lieu. Soit la mémoire A contient déjà M éléments. Dans ce dernier cas, elle place sur sa sortie 23 l'élément le plus ancien et elle l'efface de sa mémoire pour mémoriser le nouvel élément J comme élément le plus récent.

La mémoire B a un comportement différent de la mémoire A. Lorsqu'un élément J est reçu sur l'entrée 30 de la mémoire B, celle-ci vérifie si elle contient déjà cet élément J. Si cela est vrai, alors la sortie 31 prend la valeur « 1 », sinon (J pas présent dans la mémoire B), la sortie 31 prend la valeur « 0 ».

Si un élément J provenant de la mémoire A est reçu sur l'entrée 32 de la mémoire B, alors deux possibilités se présentent : soit le signal 31 est « vrai » (valeur « 1 ») soit le signal 31 est « faux » (valeur « 0 »).

Si le signal 31 est « vrai », alors le nouvel élément reçu sur l'entrée 32 de la mémoire B remplace l'élément dont la valeur est présente sur l'entrée 30 (qui est déplacé vers la mémoire A).

Si le signal 31 est « faux », il existe encore deux possibilités : soit la mémoire B contient moins de P éléments et elle mémorise le nouvel élément J ; soit la mémoire B contient déjà P éléments, c'est à dire qu'elle est pleine. Dans ce dernier cas, elle sélectionne de manière aléatoire un élément déjà mémorisé

dans la mémoire B et elle l'efface pour mémoriser à la place le nouvel élément reçu sur son entrée 32.

La mémoire B se vide donc de manière aléatoire. Un pirate qui souhaiterait éliminer un élément du dispositif de mémorisation 5 devrait donc faire beaucoup plus de tentatives que dans le cas d'une simple mémoire de type FIFO. En effet, si la taille globale de la mémoire est de N éléments, un pirate devra effectuer en moyenne bien plus de N tentatives pour éliminer un élément de la mémoire.

On notera que les mémoires A et B qui sont représentées de manière séparée sur la figure unique peuvent en réalité être deux sous-ensembles d'une même mémoire physique.

L'invention ne se limite pas à l'exemple de réalisation qui vient d'être décrit. En variante, le dispositif de mémorisation 5 peut en effet comporter une mémoire A de taille nulle. Dans une autre variante, on permet à un utilisateur de présenter un nombre déterminé de fois chaque élément au dispositif de mémorisation. Par exemple, si ce dispositif est intégré dans un appareil d'enregistrement, et que l'on autorise cet appareil à réaliser un nombre x de copies de chaque contenu, on stockera dans la mémoire, avec chaque identifiant de contenu déjà enregistré par l'appareil, le nombre y de fois où le contenu a été présenté à l'appareil pour enregistrement. Lorsque le nombre y de présentation d'un contenu donné atteint le nombre x, alors il n'est plus possible d'enregistrer ce contenu et le dispositif de mémorisation 5 retournera une information correspondante à l'appareil d'enregistrement.

REVENDICATIONS

1. Dispositif (5) de mémorisation d'une liste d'éléments destiné à mémoriser tout élément (J) qui lui a été présenté en dernier lieu et comprenant une première mémoire (3), caractérisé en ce qu'il comporte en outre des moyens chargés, lorsque la première mémoire est pleine et qu'un nouvel élément doit être mémorisé, de sélectionner aléatoirement un élément mémorisé dans la première mémoire pour effacer cet élément sélectionné et pour mémoriser le nouvel élément présenté.

2. Dispositif selon la revendication 1 capable de mémoriser N éléments, N étant un entier naturel, caractérisé en ce qu'il comporte en outre une deuxième mémoire (2) destinée à mémoriser en permanence les M éléments qui ont été présentés en dernier lieu audit dispositif, M étant un entier naturel inférieur à N,

la première mémoire (3) étant destinée à mémoriser les N-M autres éléments.

3. Dispositif selon l'une des revendications 1 ou 2, caractérisé en ce qu'il est en outre adapté à fournir une information indiquant si l'élément (J) qui lui a été présenté en dernier lieu est déjà présent dans ledit dispositif.

4. Dispositif selon l'une des revendications 1 à 3, caractérisé en ce qu'il ne contient qu'un seul exemplaire de chaque élément mémorisé.

5. Dispositif selon l'une des revendications précédentes, caractérisé en ce qu'il mémorise en outre, avec chaque élément, le nombre de fois où cet élément lui a été présenté.

6. Dispositif selon la revendication 5, caractérisé en ce qu'il est adapté à fournir une information indiquant si l'élément qui lui a été présenté en dernier lieu lui a déjà été présenté un nombre de fois qui dépasse un nombre prédéterminé.

7. Procédé de mémorisation d'un élément (J) dans un dispositif (5) selon l'une des revendications 2 à 4, caractérisé en ce qu'il comprend les étapes consistant à

(a) recevoir un élément (J) qui est présenté au dispositif (5) ;

(b) vérifier si ledit élément (J) est déjà présent dans ledit dispositif (5) ; et

- en cas de vérification positive, désigner ledit élément (J) comme élément mémorisé en dernier lieu, et
- en cas de vérification négative, mémoriser ledit élément (J) dans le dispositif.

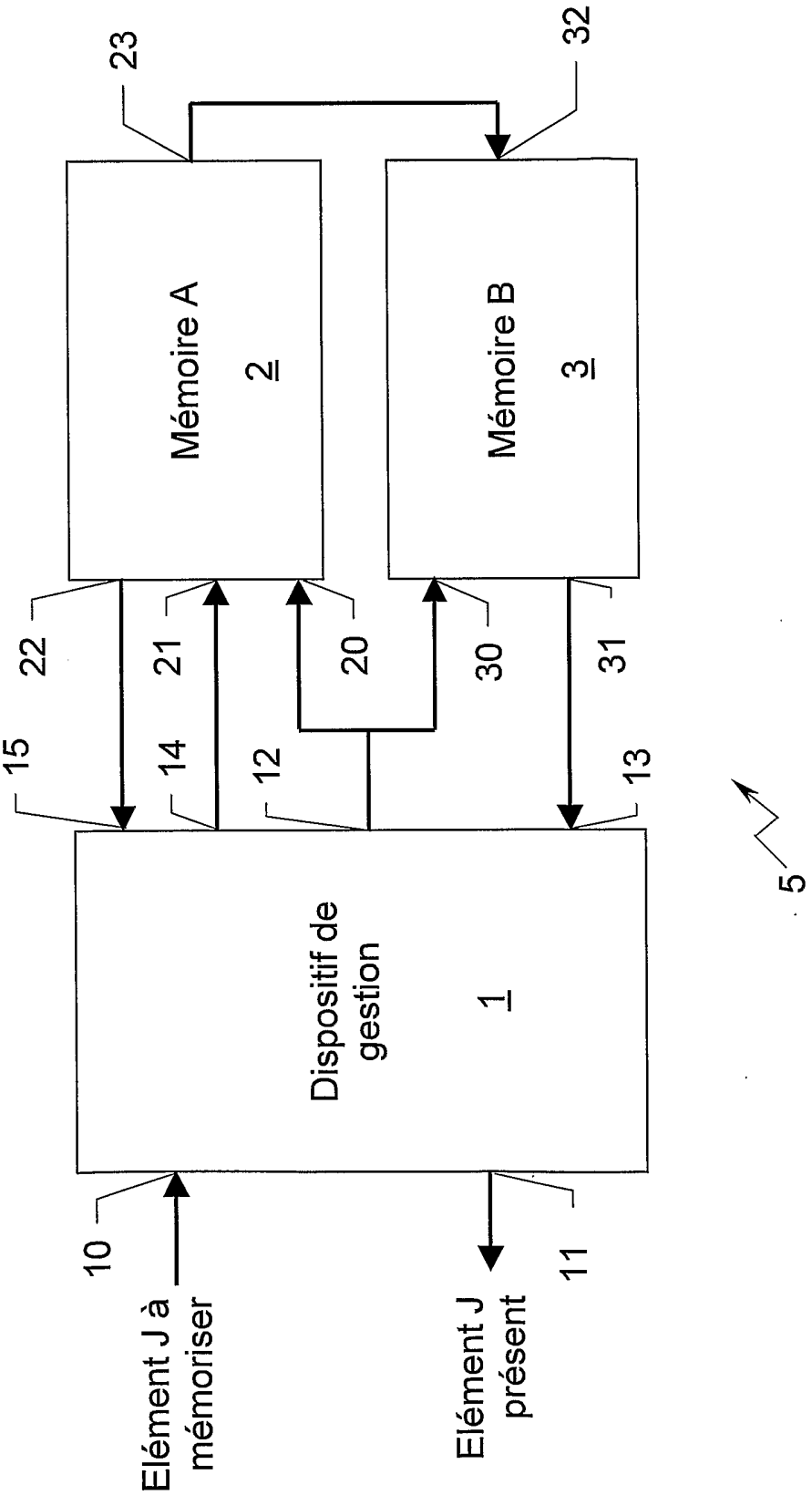
8. Procédé selon la revendication 7, caractérisé en ce qu'en cas de vérification négative à l'étape (b) :

- si la deuxième mémoire (2) n'est pas pleine, l'élément reçu (J) est mémorisé dans la deuxième mémoire (2) ; et
- si la deuxième mémoire (2) est pleine :

i) l'élément le plus ancien mémorisé dans ladite deuxième mémoire est transféré vers la première mémoire (3) ; et

ii) l'élément reçu (J) est mémorisé dans la deuxième mémoire (2) ; et

iii) si la première mémoire (3) est pleine, alors un élément mémorisé dans ladite première mémoire est sélectionné aléatoirement pour être effacé de sorte que l'élément le plus ancien mémorisé dans ladite deuxième mémoire puisse être transféré vers ladite première mémoire (3).


23
32
Mémoire A
2
Mémoire B
3
22
21
20
30
31
15
14
12
13
5
Dispositif de gestion
1
10
11
Elément J à mémoriser
Elément J présent