

(19)



(11)

EP 1 570 451 B1

(12)

FASCICULE DE BREVET EUROPEEN

(45) Date de publication et mention
de la délivrance du brevet:
27.02.2019 Bulletin 2019/09

(51) Int Cl.:
G08G 1/054 (2006.01)

(21) Numéro de dépôt: **03789477.1**

(86) Numéro de dépôt international:
PCT/FR2003/003462

(22) Date de dépôt: **24.11.2003**

(87) Numéro de publication internationale:
WO 2004/051596 (17.06.2004 Gazette 2004/25)

(54) **PROCEDES D'AUTHENTIFICATION D'IMAGES**

SYSTEM ZUR AUTHENTIFIZIERUNG VON BILDDATEN

IMAGE AUTHENTICATING METHODS

(84) Etats contractants désignés:
**AT BE BG CH CY CZ DE DK EE ES FI FR GB GR
HU IE IT LI LU MC NL PT RO SE SI SK TR**

(30) Priorité: **26.11.2002 FR 0214794**

(43) Date de publication de la demande:
07.09.2005 Bulletin 2005/36

(73) Titulaire: **Cynove**
75005 Paris (FR)

(72) Inventeurs:
• **LEWINER, Jacques**
F-92210 Saint-Cloud (FR)
• **JAVELOT, Sylvain**
F-75013 Paris (FR)

- **LEBRUN, Damien**
F-78800 Houilles (FR)
- **DEBUSNE, Stéphane**
F-92120 Montrouge (FR)
- **FRANCOIS, Jean-Philippe**
F-75001 Paris (FR)

(74) Mandataire: **A.P.I. Conseil**
Technopôle Hélioparc
2, Avenue Pierre Angot
64053 Pau Cedex 09 (FR)

(56) Documents cités:
EP-A- 0 621 572 EP-A2- 1 001 601
WO-A-02/082400 WO-A1-02/32031
US-B1- 6 269 446 US-B1- 6 415 042

EP 1 570 451 B1

Il est rappelé que: Dans un délai de neuf mois à compter de la publication de la mention de la délivrance du brevet européen au Bulletin européen des brevets, toute personne peut faire opposition à ce brevet auprès de l'Office européen des brevets, conformément au règlement d'exécution. L'opposition n'est réputée formée qu'après le paiement de la taxe d'opposition. (Art. 99(1) Convention sur le brevet européen).

Description

[0001] La présente invention est relative aux procédés permettant l'authentification d'images et notamment celles de véhicules pris en infraction, de telles infractions pouvant par exemple être relatives à un dépassement des vitesses autorisées, à un franchissement de feux rouges ou encore à la circulation d'un véhicule non autorisé dans une voie réservée aux véhicules de transport en commun.

[0002] En effet, jusqu'à présent, deux méthodes de contrôle sont utilisées, à savoir des méthodes nécessitant des interventions humaines lors de la constatation de l'infraction ou des méthodes semi-automatiques avec saisie de l'image des véhicules en infraction.

[0003] Dans le premier cas, les contrôles de vitesse nécessitent l'intervention physique de forces de l'ordre qui en général et dans un premier temps constatent l'infraction.

[0004] Le procès-verbal résultant de ce constat est ensuite exploité pour sanctionner l'infraction et le cas échéant mettre en oeuvre des moyens pour faire payer au conducteur en infraction les amendes correspondantes.

[0005] Toutefois, une telle suite d'opérations requiert des interventions humaines à tous les stades du processus.

[0006] Ainsi, la probabilité d'un contrôle de vitesse reste relativement faible et la lourdeur des traitements ultérieurs des procès-verbaux conduit à un taux d'encaissement des amendes assez faible.

[0007] Ceci a pour conséquence de donner l'impression à certains automobilistes d'un sentiment d'impunité, ce qui est négatif en termes de sécurité.

[0008] Le même problème se pose pour des infractions de natures différentes, par exemple, le franchissement d'un feu rouge ou la circulation dans une voie réservée.

[0009] Dans le second cas, la mise en place de procédures automatisées allant de la constatation de l'infraction jusqu'à la récupération des sommes réclamées au titre des amendes semble de nature à grandement améliorer la sécurité et le respect des règles de circulation.

[0010] Plusieurs approches ont été proposées dans le passé pour tenter d'automatiser de telles procédures.

[0011] Par exemple, il a été proposé dans le brevet US 5,381,155 d'utiliser un radar à effet Doppler pour, dans un premier temps mesurer la vitesse des véhicules et ainsi pouvoir constater s'ils sont en infraction, puis déclencher une caméra de façon à saisir des images du ou des véhicules en infraction.

[0012] Ces images sont alors transmises à une unité de calcul pour permettre la reconnaissance et l'identification des plaques d'immatriculation des véhicules en question, puis les images peuvent alors être stockées dans des mémoires non volatiles.

[0013] Lorsque les dites plaques d'immatriculation ont été identifiées, il est alors possible de transmettre les

numéros d'immatriculation des véhicules en infraction par les systèmes de télécommunications réservés aux forces de l'ordre et ainsi de permettre l'intervention de ces dernières.

5 **[0014]** La présence de représentants des forces de l'ordre est alors nécessaire pour la constatation de l'infraction.

10 **[0015]** En cas de contestation de l'infraction par le ou les conducteurs concernés, les images enregistrées au moment de l'infraction peuvent être extraites de la mémoire dans laquelle elles ont été stockées et être exploitées.

[0016] Une telle approche se heurte toutefois à un obstacle majeur.

15 **[0017]** Il est en effet aisé, par exemple en utilisant un logiciel de retouche graphique, de modifier les images stockées et de remplacer, par exemple, les numéros des plaques d'immatriculation par d'autres.

20 **[0018]** Dès lors qu'une telle manipulation peut être facilement mise en oeuvre, la valeur légale des images transmises est largement réduite.

[0019] EP 0 621 572 A1 divulgue également un procédé d'authentification d'image comportant des moyens d'encryptage et de compression d'images. Afin de tenter de remédier à cet inconvénient il a été proposé par exemple

25 dans les brevets WO 02 08400 A et EP 0 621 572 A de crypter les images afin de rendre difficile toute manipulation.

30 **[0020]** Une telle approche présente toutefois de graves inconvénients.

[0021] En effet, la diffusion de ces images n'est alors permise qu'aux seules forces de l'ordre accédant aux algorithmes de décryptage et en aucun cas au contrevenant en cas de contestation par ce dernier.

35 **[0022]** De plus, une fois les images décryptées, leur altération est à nouveau possible et la valeur légale des images transmises est à nouveau fortement réduite.

[0023] Afin de tenter d'éviter ces inconvénients, il a été proposé dans le brevet US 5,563,590 d'insérer dans l'image prise au moment de l'infraction, des informations relatives à la vitesse du véhicule, l'heure et lieu de l'infraction, etc. sous forme de caractères alphanumériques.

40 **[0024]** A partir des informations alphanumériques ainsi recueillies on construit de nouveaux caractères alphanumériques de contrôle qui sont également insérés à l'image.

45 **[0025]** Les photographies correspondantes aux véhicules en infraction contiennent à la fois les informations caractéristiques ci-dessus et les caractères alphanumériques de contrôle.

[0026] Ultérieurement, en cas de contestation de ces documents, il est possible de vérifier que les caractères alphanumériques de contrôle sont bien ceux qui correspondaient aux informations caractéristiques prises lors

55 de l'infraction.

[0027] Toutefois, le dispositif décrit dans ce brevet présente des inconvénients importants, de diverses natures.

[0028] En particulier, il utilise des techniques de pho-

tographie argentique qui nécessitent un développement chimique des films.

[0029] Ceci entraîne un besoin d'interventions humaines régulières et coûteuses, par exemple pour charger les bobines de films dans les caméras et les remplacer lorsqu'elles ont été utilisées.

[0030] La simple utilisation de supports de stockages numériques en lieu et place des supports argentiques ne résout en rien ces problèmes.

[0031] En effet, les caractères alphanumériques utilisés pour caractériser les images et assurer leur contrôle apparaissent dans ce cas de manière directement identifiable sur les images et il est relativement facile de les modifier, par exemple à l'aide du logiciel de retouche graphique précédent.

[0032] En outre, ces informations occultent une partie de l'image ce qui peut donner lieu à contestations dans certains cas.

[0033] Dans un autre perfectionnement il a été proposé dans le brevet US 6,269,446 de calculer une signature numérique à partir des images, cette signature étant placée de façon cachée et non standardisée, dans l'entête des fichiers d'images.

[0034] Cette solution présente toutefois au moins trois graves inconvénients :

- premièrement, certains formats de fichiers d'image ne possèdent pas d'entête, en particulier la plupart des fichiers représentatifs d'images enregistrées sans traitement du type des compressions d'images, c'est à dire ceux apportant la meilleure définition,
- deuxièmement, la signature en question étant masquée, elle peut être contestée par les automobilistes en infraction car elle ne fait pas partie intégrante des éléments du dossier juridique de l'infraction,
- enfin, en raison du caractère non standardisé de ces opérations cette signature peut se trouver effacée de façon irréversible lors de simples opérations de sauvegarde des fichiers.

[0035] La présente invention a notamment pour but de proposer un procédé d'authentification d'images et notamment d'images de véhicules pris en infraction et à cette fin, un procédé selon l'invention comporte les étapes suivantes :

- on répartit des systèmes de prises de vues, agencés de manière à permettre la prise d'images et la saisie des éléments d'identification des contrevenants, les moyens de prises de vues fournissant des données représentatives des images prises, ci après appelées données d'images prises,
- on prévoit des moyens, ci-après appelés systèmes informatiques, déclenchés pour la saisie des informations physiques relatives à l'infraction, mesure de la

vitesse, temps, date, lieu, etc. ci-après appelées données d'infraction,

- on prévoit des premiers moyens de mémorisation et/ou de transmission des données d'images prises et des données d'infraction,
- on prévoit, des systèmes d'exploitation pour exploiter les données mémorisées et/ou transmises,

et est essentiellement caractérisé en ce que :

- les systèmes d'exploitation appliquent aux données d'images prises, tout traitement connu propre à améliorer ou conserver la qualité des images en question et/ou à réduire le nombre de données nécessaires à une reconstitution de ces images, sans perte significative de leur qualité, afin de réduire la taille des mémoires nécessaires pour stocker les données d'images prises et/ou la capacité des moyens de transmission de ces données, les données intermédiaires représentatives d'images après ces traitements étant appelées données initiales graphiques,
- les systèmes d'exploitation calculent, à partir des données d'infraction et d'une représentation graphique des caractères alphanumériques associés à ces données d'infraction, de nouvelles données représentatives d'images, appelées données d'infraction graphiques,
- les systèmes d'exploitation fusionnent les données initiales graphiques et les données d'infraction graphiques de façon à obtenir un nouvel ensemble de données représentatives d'images, appelées données identifiantes graphiques, dans lequel les données initiales graphiques et les données d'infraction graphiques constituent des sous-ensembles accessibles de ce nouvel ensemble de données,
- les systèmes d'exploitation calculent, par application aux données identifiantes graphiques d'une fonction non-bijective notée f , un ensemble de données, ci-après appelées données résumées, de telle sorte que la connaissance des seules données résumées, ne permette pas de remonter aux données identifiantes graphiques,
- les systèmes d'exploitation appliquent aux données résumées un procédé de codage noté c , possédant un procédé de décodage associé noté c^{-1} , pour obtenir un nouvel ensemble de données appelées données signatures,
- les systèmes d'exploitation calculent, à partir des données signatures et d'une représentation graphique des caractères alphanumériques associés à ces données signatures, de nouvelles données repré-

sentatives d'images, appelées données signatures graphiques,

- les systèmes d'exploitation fusionnent les données identifiantes graphiques et les données signatures graphiques de façon à obtenir un nouvel ensemble de données représentatives d'images, dans lequel les données identifiantes graphiques et ces données signatures graphiques constituent des sous-ensembles accessibles de ce nouvel ensemble de données, appelées données authentifiables graphiques,
- on prévoit des seconds moyens de mémorisation et/ou de transmission des données authentifiables graphiques,
- on prévoit des unités de contrôle qui peuvent respectivement lire et/ou recevoir les données authentifiables graphiques stockées dans les seconds moyens de mémorisation et/ou de transmission, les données effectivement lues et/ou reçues étant appelées données reçues graphiques,
- les unités de contrôle recherchent parmi les données reçues graphiques le sous-ensemble des données identifiantes graphiques, ci-après appelées données identifiantes graphiques testées,
- les unités de contrôle recherchent parmi les données reçues graphiques, le sous-ensemble des données signatures graphiques, ci-après appelées données signatures graphiques testées,
- les unités de contrôle recherchent à partir des données signatures graphiques testées et d'une table de reconnaissance des caractères alphanumériques, un ensemble de données représentatif des données signatures, appelées données signatures testées,
- les unités de contrôle calculent par l'application, aux données identifiantes graphiques testées, de la fonction f non-bijective, un ensemble de données, appelées données résumées testées,
- les unités de contrôle appliquent aux données signatures testées, le procédé de décodage c^{-1} pour obtenir un ensemble de données, appelées données résumées reçues,

et les unités de contrôle comparent les données résumées reçues et les données résumées testées, et fournissent un signal d'alerte lorsque ces données ne sont pas identiques et/ou un signal de confirmation lorsqu'elles le sont.

[0036] Dans des modes de réalisations préférés du procédé selon l'invention, on a recours en outre à l'une

et/ou à l'autre des dispositions suivantes :

- les systèmes informatifs comportent des moyens de mesure de la vitesse de véhicules,
- les systèmes informatifs comportent des moyens de détection de la présence d'un véhicule non autorisé dans une voie réservée,
- les systèmes informatifs comportent des moyens de détection du franchissement d'un feu rouge par un véhicule,
- les systèmes de prises de vues fournissent des images numériques,
- les procédés de codage et/ou décodage utilisent des techniques cryptographiques,
- les procédés de codage incorporent dans les données signatures, un sous-ensemble de données, sous-ensemble accessible et contenant l'ensemble des caractères alphanumériques suffisants pour représenter les données signatures,
- les systèmes d'exploitation appliquent aux données d'images prises, successivement un procédé de compression et le procédé de décompression associé, et mémorisent et/ou transfèrent les données obtenues vers des moyens de mémorisation et/ou de transmission,
- les premiers moyens de mémorisation et/ou de transmission et les seconds moyens de mémorisation et/ou de transmission sont confondus,
- la table de reconnaissance des caractères est élaborée par application d'un code programme de reconnaissance des caractères,
- la table de reconnaissance des caractères est élaborée à partir des données signatures graphiques testées.

[0037] L'objet de l'invention peut être obtenu par un procédé d'authentification d'images et notamment d'images de véhicules pris en infraction selon la revendication 1. D'autres caractéristiques et avantages de l'invention apparaîtront au cours de la description détaillée suivante d'une de ses formes de réalisation, donnée à titre d'exemple non limitatif en regard des dessins joints.

[0038] Sur les dessins :

- la figure 1 est une vue schématique d'un procédé selon l'art antérieur où un véhicule (1) en déplacement sur la chaussée (100) selon la direction indiquée par la flèche (F), est intercepté par le faisceau radar (200) d'un système informatif comportant no-

tamment un cinémomètre (2), relié à des systèmes d'exploitation (4), et à des systèmes de prises de vues (3),

- la figure 2 est une vue schématique d'une étape du procédé selon l'invention où un processeur (400) des systèmes d'exploitation fusionne les données initiales graphiques (10), d'un véhicule (1) pris de face et comportant des éléments d'identification (101) et les données d'infraction graphiques (11), pour obtenir les données identifiantes graphiques (12),
- la figure 3 est une vue schématique d'une étape intermédiaire du procédé selon l'invention où un processeur (400) des systèmes d'exploitation calcule à partir des données identifiantes graphiques (12) et par action d'un code programme (40) approprié placé dans un moyen de mémorisation non volatile, les données résumées (31),
- la figure 4 est une vue schématique d'une étape intermédiaire du procédé selon l'invention où un processeur (400) des systèmes d'exploitation (4) calcule à partir des données résumées (31) et par action d'un code programme approprié (41) placé dans un moyen de mémorisation non volatile, les données signatures (33),
- la figure 5 est une vue schématique d'une étape intermédiaire d'un procédé selon l'invention où un processeur (400) des systèmes d'exploitation (4) fusionne les données identifiantes graphiques (12) et les données signatures graphiques (13), pour constituer les données authentifiables graphiques (14),
- la figure 6 est une vue schématique représentant un exemple de suite d'étapes du procédé selon l'invention, les systèmes d'exploitation et les unités de contrôle, ici placés en extérieur pour ne pas alourdir la figure, étant connectés par tout moyen connu aux différents éléments.

[0039] Lorsque la vitesse d'un véhicule (1), comportant un élément d'identification (101), telle qu'une plaque d'immatriculation, excède la limite de vitesse autorisée, un dispositif selon l'art antérieur comportant un cinémomètre (2) et un système de prises de vues (3) est agencé pour prendre des images du véhicule en infraction, de façon à permettre son identification.

[0040] Le cinémomètre peut être par exemple constitué à partir d'un radar à effet Doppler, de boucles magnétiques enterrées sous la chaussée ou d'un système laser.

[0041] Des moyens sont prévus pour fournir des informations physiques associées, telles que l'heure et la date de l'infraction, l'emplacement du dispositif, etc.

[0042] Des premiers moyens sont prévus pour enregistrer et/ou transmettre les données représentatives

des images prises par les systèmes de prises de vues, ci-après désignées données d'images prises (30) et les données représentatives des informations physiques, ci-après appelées données d'infraction (20), préférentiellement sous forme de données numériques.

[0043] Dans l'exemple de la figure 6, on a placé des moyens de mémorisation et/ou transmission en 3 points du schéma, mais de tels moyens peuvent évidemment être prévus en tout autre point de ce schéma aux endroits naturellement déterminés de manière connue en soi par tout homme de l'art.

[0044] Les moyens de mémorisation peuvent également être réalisés de toute manière connue en utilisant par exemple des mémoires à semi-conducteurs, magnétiques, etc.

[0045] Les moyens de transmission des données peuvent être de diverses natures : transmission par fil, par bus de communication ou par radio.

[0046] Des systèmes d'exploitation (4) sont prévus pour exploiter ces données.

[0047] Afin notamment de réduire les durées de transmission des données d'infraction et des données d'images prises et/ou pour effectuer les divers traitements mis en oeuvre dans le procédé, il est avantageux de doter les systèmes d'exploitation d'un ou plusieurs processeurs (400) et de premiers moyens de mémorisation volatile et non volatile et/ou de transmission (430A).

[0048] Dans des exemples particuliers de réalisation, les processeurs peuvent être intégrés dans des composants semi-conducteurs de type FPGA ou des composants semi-conducteurs spécialisés de type ASIC.

[0049] Le contenu de ces premiers moyens de mémorisation peut être évidemment lu et écrit par les processeurs de ces systèmes d'exploitation.

[0050] De manière connue en soi, il est possible d'appliquer aux données recueillies des procédés de compression des données permettant de réduire la taille des mémoires utilisées pour leur stockage ou la capacité des moyens de transmission de ces données.

[0051] Parmi les procédés de compression des données, il est possible d'utiliser des procédés dits sans perte d'information ou des procédés dits entropiques, avec pertes d'informations, particulièrement appliqués aux données représentatives d'images, et ainsi d'obtenir des données compressées.

[0052] On choisit alors, un facteur de compression permettant l'identification sans ambiguïté des véhicules pris en infraction lors de la visualisation de ces images.

[0053] Le choix du facteur de compression peut être fait par exemple lors de l'installation des systèmes de prises de vues, les systèmes d'exploitation enregistrant dans les moyens de mémorisation les données représentatives d'images prises pour différents facteurs de compression, et transmettant le contenu de ces moyens de mémorisation à des unités de contrôle (5), utilisées à titre exceptionnel pendant cette phase d'installation.

[0054] Ces unités de contrôle disposent de moyens de visualisation afin de vérifier la qualité des images recons-

tituées à partir de ces données compressées.

[0055] De même, lorsque cela est nécessaire, par exemple en cas de mauvaises conditions d'éclairage ou d'intempéries, les systèmes d'exploitation peuvent appliquer tout traitement connu aux données d'images prises afin de faciliter l'identification des véhicules en infraction.

[0056] Par exemple et de manière connue, il est possible renforcer le contraste de ces images et de reconnaître les caractères alphanumériques inscrits sur la plaque d'immatriculation.

[0057] Après l'application éventuelle de ces traitements, on obtient de nouvelles données représentatives d'images des véhicules en infraction appelées données initiales graphiques (10) qui peuvent être mémorisées et/ou transmises.

[0058] Tout procédé connu de mémorisation peut être utilisé, et en particulier des procédés non volatils.

[0059] Des moyens de mémorisation non volatile sont utilisés pour stocker la représentation graphique des caractères alphanumériques issus des systèmes informatiques, ces moyens de mémorisation étant appelés mémoire non volatile des polices de caractères (410).

[0060] Dans un premier exemple de réalisation, la mémoire non volatile des polices de caractères contient la représentation graphique des caractères alphanumériques sous forme de matrices de points.

[0061] Dans un second exemple de réalisation, la mémoire non volatile des polices de caractères contient la représentation graphique des caractères alphanumériques sous forme de codes barres.

[0062] On détermine à partir des données d'infraction et de la représentation graphique des caractères alphanumériques, de nouvelles données représentatives d'images visualisant les données d'infraction, ces images étant par exemple :

123 km/h -01/01/02-

10h:30- Paris Aima

tel qu'illustré sur la figure 2, ces données étant appelées par la suite données d'infraction graphiques (11).

[0063] Dans le cas particulier où on n'a pas appliqué de procédé de compression aux données d'images prises et où on souhaite pouvoir visualiser simultanément l'image du véhicule pris en infraction et les images visualisant les données d'infraction, on élabore un nouvel ensemble de données, appelées données identifiantes graphiques (12) par les étapes suivantes :

- on détermine les dimensions relatives des images des données représentatives des images incorporant les données initiales graphiques et les données d'infraction graphiques, cette opération ayant d'ailleurs pu être faite lors de l'installation du système,
- et on enregistre dans une mémoire les données initiales graphiques et les données d'infraction graphiques.

[0064] Sur la figure 6, les traits pointillés dans les moyens de mémorisation et/ou transmission (430A) sont une représentation symbolique du fait que les données d'infraction graphiques sont issues des données d'infraction (20) et que les données initiales graphiques sont issues des données d'images prises (30).

[0065] De cette manière, les données d'infraction graphiques et les données initiales graphiques constituent bien deux sous-ensembles accessibles des données identifiantes graphiques.

[0066] Sur l'exemple particulier représenté sur la figure 2, les images représentant les données de l'infraction sont placées sous les images prises par les systèmes de prises de vue.

[0067] Il va de soi, que ces images représentant les données d'infraction pourraient de façon équivalente être, par exemple, placées au-dessus des images prises par les systèmes de prises de vues, ou sur les côtés ou de toute autre manière.

[0068] Il est à noter que lorsqu'un de procédé de compression des données a été utilisé, la fusion des données identifiantes graphiques et des données d'infraction graphique est également possible.

[0069] Dans ce cas, il est par exemple possible d'appliquer dans une étape intermédiaire le procédé de décompression associé aux deux ensembles de données, ce qui permet de se ramener au cas précédent, puis d'appliquer une nouvelle fois le procédé de compression pour obtenir les données identifiantes graphiques.

[0070] Un code programme (40) nécessaire à l'application à un ensemble de données choisies, d'un procédé de calcul non bijectif connu de l'art antérieur ci-après appelé fonction f, est mémorisé dans une mémoire non volatile.

[0071] Par exemple, il est possible d'utiliser le procédé de calcul décrit dans le document de standardisation FIPS PUB 180-1, publié par le National Technical Information Service, U.S. Department of Commerce, Springfield CA 22161.

[0072] La mise en oeuvre de ce procédé aux données identifiantes graphiques conduit à un nouvel ensemble de données ci après appelées données résumées (31).

[0073] Dans le cas ci-dessus, les données résumées sont alors des ensembles de 160 bits d'information.

[0074] Il est à noter, qu'avec des images dont la définition permet l'identification des véhicules en infraction, c'est à dire comportant plusieurs dizaines de milliers d'éléments d'image, il est évidemment impossible, à partir des données résumées de 160 bits, de reconstituer les données identifiantes graphiques en utilisant un procédé de calcul inverse.

[0075] On applique alors aux données résumées un procédé de chiffrement dit à clé publique/clé privée, tel que décrit par exemple dans le brevet US 4,405,829, ce qui conduit à de nouvelles données, ci-après désignées données résumées codées (32).

[0076] Là encore, le code programme (41) nécessaire à l'application du procédé de chiffrement en question est

mémorisé dans une mémoire non volatile.

[0077] La clé privée ci-dessus est connue des seuls personnels habilités.

[0078] La clé privée peut être mémorisée dans les systèmes d'exploitation de manière permanente ou préférentiellement dans des mémoires volatiles, ce qui permet d'améliorer la sécurité du procédé.

[0079] Dans ce dernier cas, cette clé peut être téléchargée à partir d'une base de données hautement sécurisée.

[0080] Ainsi, en cas de vol d'un dispositif mettant en oeuvre le procédé, la clé privée reste inaccessible, même en cas d'analyse des éléments constitutifs du dispositif.

[0081] Dans un exemple particulier de réalisation, les systèmes d'exploitation fusionnent les données résumées codées avec un autre ensemble de données, appelées données d'alphabet (420), par exemple en plaçant à la suite des données résumées codées l'ensemble des caractères alphanumériques suffisant pour représenter les données résumées codées.

[0082] Par exemple, lorsque les données résumées codées sont représentées dans une base hexadécimale, les systèmes d'exploitation placent à la suite des données résumées codées, les caractères alphanumériques 0 à 9 et A à F qui constituent dans ce cas les données d'alphabet.

[0083] Il est à noter que dans l'exemple particulier de mise en oeuvre du procédé ci-dessus, les données d'alphabet sont placées à la suite des données résumées codées, mais que ces données d'alphabet pourraient être placées de façon équivalente avant ces données résumées codées ou de toute autre manière permettant de reconstituer l'intégralité du sous-ensemble des données d'alphabet.

[0084] Les données résumées codées, éventuellement fusionnées avec les données d'alphabet, sont appelées données signatures (33).

[0085] Il est également à noter que la fusion des données d'alphabet avec les données résumées codées ne modifie en rien l'existence du procédé de décodage c^{-1} , puisque les données résumées codées constituent toujours un sous-ensemble accessible de ces données signatures.

[0086] On détermine alors à partir des données signatures et de la représentation graphique des caractères alphanumériques, de nouvelles données représentatives d'images visualisant les données signatures, ces images étant par exemple : 13579BDF02468ACE1357

[0087] tel qu'illustré sur la figure 5, ces nouvelles données étant appelées par la suite données signatures graphiques (13).

[0088] Les représentations graphiques en question peuvent être constituées de matrices de points ou de codes barres par exemple.

[0089] On fusionne alors les données identifiantes graphiques (12) avec les données signatures graphiques (13), par exemple, selon le procédé déjà utilisé pour fusionner les données d'infraction graphiques (11) avec

les données initiales graphiques (10) et l'on obtient ainsi les données authentifiables graphiques (14).

[0090] Sur l'exemple particulier de la figure 5, les images représentant les données signatures sont placées sous les images représentant les données identifiantes graphiques. Il va de soi, que ces images représentant les données signatures pourraient de façon équivalente être, par exemple, placées au-dessus des images représentant les données identifiantes graphiques, ou sur les côtés ou de toute autre manière.

[0091] Les systèmes d'exploitation sont en outre dotés de seconds moyens de mémorisation et/ou de transmission (430B) afin de permettre la diffusion des données authentifiables graphiques.

[0092] Dans un premier exemple de réalisation, les systèmes d'exploitation comportent ces seconds moyens de mémorisation non volatile, sous forme amovibles, par exemple sous forme d'une carte mémoire qui peut être retirée du système par un opérateur et placée dans une unité de contrôle (5).

[0093] Une telle unité de contrôle peut être constituée d'un ordinateur portable ou d'un boîtier beaucoup plus petit apte à relire le contenu de la carte lorsqu'elle lui est associée.

[0094] Dans ce premier exemple de réalisation, ces moyens de mémorisation non volatile amovibles peuvent également être utilisés comme premiers moyens de mémorisation.

[0095] Dans un second exemple de réalisation, les systèmes d'exploitation comportent des moyens de télécommunication par exemple, reliés à une ligne téléphonique, de façon à permettre la transmission des données authentifiables graphiques vers une unité de contrôle.

[0096] Une telle unité de contrôle peut être constituée d'un ordinateur muni d'un modem connecté à une ligne téléphonique.

[0097] Dans ce second exemple de réalisation, ces moyens de transmission peuvent également être utilisés comme premiers moyens de transmission pour la télécommunication avec les systèmes de prises de vues.

[0098] Dans un troisième exemple de réalisation, les systèmes d'exploitation comportent des moyens de télécommunication sans fil et sont agencés pour transmettre les données authentifiables graphiques à une unité de contrôle.

[0099] L'unité de contrôle peut être constituée d'un ordinateur comprenant un modem radio.

[0100] Dans ce troisième exemple de réalisation, les premiers moyens de transmission peuvent être de même nature que ceux ci-dessus.

[0101] Les données effectivement lues et/ou reçues par les unités de contrôle sont appelées données reçues graphiques (50).

[0102] Les unités de contrôle comportent un ou plusieurs processeurs.

[0103] Les unités de contrôle peuvent enregistrer dans des troisièmes moyens de mémorisation (530A), comme

des disques durs par exemple, les données reçues graphiques sous la forme de fichiers informatiques.

[0104] Ces moyens de mémorisation peuvent être utilisés également pour contenir tous les algorithmes et données nécessaires à la recherche des dimensions et positions des données identifiantes graphiques et des données signatures graphiques.

[0105] On sépare alors l'ensemble des données reçues graphiques en deux sous-ensembles de données appelées données identifiantes graphiques testées (51) et données signatures graphiques testées (52), ces deux sous-ensembles étant respectivement associés aux sous-ensembles des données identifiantes graphiques et des données signatures graphiques de l'ensemble des données mémorisées et/ou transmises par les systèmes d'exploitation.

[0106] Dans un premier exemple de réalisation, les unités de contrôle comportent dans les moyens de mémorisation non volatile, un code programme de reconnaissance (510A) des caractères qui convertit les données signatures graphiques testées, en caractères alphanumériques pour former un nouvel ensemble de données appelées données signatures testées.

[0107] Dans un second exemple de réalisation et lorsque les données résumées codées ont été fusionnées comme décrit plus haut avec les données d'alphabet (420), pour former les données signatures, on effectue au niveau des unités de contrôle les étapes suivantes :

- on recherche les données signatures graphiques testées dans les données reçues graphiques,
- on recherche les représentations graphiques des données d'alphabet dans les données signatures graphiques, appelées données d'alphabet graphiques testées (510B),
- on calcule les données signatures testées (53) en comparant les données signatures graphiques testées avec les données d'alphabet graphiques testées.

[0108] Les moyens de mémorisation peuvent également contenir le code programme d'exécution du calcul non-bijectif utilisé plus haut, défini par la fonction f , ainsi que le code programme d'exécution du programme de décodage c^{-1} , connu grâce à la clé publique associée à la clé privée qui a été utilisée pour coder les données résumées.

[0109] On applique respectivement la fonction f aux données identifiantes graphiques testées (51) ce qui conduit à de nouvelles données appelées données résumées testées (55) et le programme de décodage c^{-1} aux données signatures testées ce qui conduit à de nouvelles données, appelées données résumées reçues (54).

[0110] On compare les données résumées testées et les données résumées reçues.

[0111] Lorsque ces deux ensembles de données sont identiques, on considère que les images ont été authentifiées.

[0112] On peut afficher sur un écran un message alphanumérique de validation directement lisible par un opérateur humain.

[0113] Au contraire lorsque ces deux ensembles de données ne sont pas identiques, on peut fournir un signal visualisable sur un écran ou par tout autre procédé qui indique qu'une manipulation d'image a été détectée.

[0114] En utilisant le procédé qui vient d'être décrit il est ainsi possible de vérifier qu'il n'y a pas eu de falsification d'une image par exemple en affectant à un véhicule en infraction des caractéristiques d'identification d'un autre véhicule.

[0115] L'authentification des images en résultant résout ainsi les problèmes non résolus présentés plus haut.

[0116] Comme il va de soi, et comme il résulte d'ailleurs de ce qui précède, l'invention n'est pas limitée à l'exemple de réalisation particulier qui vient d'être décrit, mais est définie par les revendications ci-jointes; elle embrasse la variante dans laquelle le procédé est mis en oeuvre lorsque l'infraction est autre que celle associée aux dépassements de vitesse autorisée par un véhicule et par exemple lorsqu'elle est relative à la détection d'une personne dans une zone d'accès protégée pour laquelle elle ne dispose pas d'une habilitation.

30 Revendications

1. Procédé d'authentification d'images et notamment d'images de véhicules pris en infraction comportant les étapes suivantes:

- on répartit des systèmes de prises de vues (3), agencés de manière à permettre la prise d'images et la saisie des éléments d'identification (101) des contrevenants (100), les moyens de prises de vues fournissant des données représentatives des images prises, ci-après appelées données d'images prises (30),
- on prévoit des moyens, ci-après appelés systèmes informatifs (2), pour la saisie des informations physiques relatives à l'infraction, ci-après appelées données d'infraction (20),
- on prévoit des premiers moyens de mémorisation et/ou de transmission (430A) des données d'images prises et des données d'infraction,
- on prévoit, des systèmes d'exploitation (4) pour exploiter les données mémorisées et/ou transmises,

et est essentiellement **caractérisé en ce que**

- a) - les systèmes d'exploitation calculent, à partir des données d'infraction et d'une représentation

graphique des caractères alphanumériques (410) constituant ces données d'infraction, de nouvelles données représentatives d'images, appelées données d'infraction graphiques (11),

b) - les systèmes d'exploitation fusionnent les données d'images prises (30) et les données d'infraction graphiques (11) de façon à obtenir un nouvel ensemble de données représentatives d'images, appelées données identifiantes graphiques (12), dans lequel les données d'images prises (30) et les données d'infraction graphiques constituent des sous-ensembles accessibles, par les processeurs constitutifs des systèmes d'exploitation, de ce nouvel ensemble (12) de données,

c) - les systèmes d'exploitation mettent en oeuvre un procédé de calcul non-bijectif, encore appelé fonction non-bijective notée f , appliqué aux données identifiantes graphiques (12) et conduisant à un ensemble de données, ci-après appelées données résumées (31), lesdites données résumées étant des ensembles de 160 bits d'information ne permettant pas de remonter aux données identifiantes graphiques (12),

d) - les systèmes d'exploitation appliquent aux données résumées (31) un procédé de codage noté c , possédant un procédé de décodage associé noté c^{-1} , pour obtenir un nouvel ensemble de données, appelées données résumées codées (32)

e) - les systèmes d'exploitation fusionnent les données résumées codées (32) avec des données alphabet (420) pour obtenir un ensemble de données, appelées données signatures (33),

f) - les systèmes d'exploitation calculent, à partir des données signatures (33) et d'une représentation graphique des caractères alphanumériques (410) constituant ces données signatures (33), de nouvelles données représentatives d'images, appelées données signatures graphiques (13),

g) - les systèmes d'exploitation fusionnent les données identifiantes graphiques (12) et les données signatures graphiques (13) de façon à obtenir un nouvel ensemble de données représentatives d'images, dans lequel les données identifiantes graphiques et ces données signatures graphiques constituent des sous-ensembles accessibles de ce nouvel ensemble de données, appelées données authentifiables graphiques (14), où les données signatures graphiques sont constituées de matrice de points ou de codes barres.

h) - on prévoit des seconds moyens de mémorisation et/ou de transmission (430B) des données authentifiables graphiques (14),

i) - on prévoit des unités de contrôle (5) qui peuvent respectivement lire et/ou recevoir les don-

nées authentifiables graphiques stockées dans les seconds moyens de mémorisation et/ou de transmission, les données effectivement lues et/ou reçues étant appelées données reçues graphiques (50),

j) - les unités de contrôle recherchent parmi les données reçues graphiques le sous-ensemble des données identifiantes graphiques, ci-après appelées données identifiantes graphiques testées (51),

k) - les unités de contrôle recherchent parmi les données reçues graphiques, le sous-ensemble des données signatures graphiques, ci-après appelées données signatures graphiques testées (52),

l) - les unités de contrôle recherchent à partir des données signatures graphiques testées et d'une table de reconnaissance (510) des caractères alphanumériques, un ensemble de données représentatif des données signatures, appelées données signatures testées (53),

m) - les unités de contrôle calculent par l'application aux données identifiantes graphiques testées, de la fonction f non-bijective, un ensemble de données, appelées données résumées testées (55),

n) - les unités de contrôle appliquent aux données signatures testées, le procédé de décodage c^{-1} pour obtenir un ensemble de données, appelées données résumées reçues (54), et

o) - les unités de contrôle comparent les données résumées reçues et les données résumées testées, et fournissent un signal d'alerte lorsque ces données ne sont pas identiques ou un signal de confirmation lorsqu'elles le sont.

2. Procédé selon la revendication 1, **caractérisé en ce que** les systèmes d'exploitation appliquent aux données d'images prises (30) :

- des procédés de compression entropiques de données permettant de réduire la taille des mémoires nécessaires pour stocker les données d'images prises et/ou la capacité des moyens de transmission de ces données, et/ou
- tout autre traitement, de type renforcement du contraste, permettant de faciliter l'identification du véhicule en infraction,
- et **en ce que** à l'issue de ces traitements, lesdites données (30) représentatives d'images sont appelées données initiales graphiques (10).

3. Procédé selon la revendication 1 ou 2 **caractérisé en ce que** les systèmes informatiques comportent des moyens de mesure de la vitesse de véhicules.

4. Procédé selon la revendication 1 ou 2 **caractérisé**

en ce que les systèmes informatiques comportent des moyens de détection de la présence d'un véhicule non autorisé dans une voie réservée.

5. Procédé selon la revendication 1 ou 2 **caractérisé en ce que** les systèmes informatiques comportent des moyens de détection du franchissement d'un feu rouge par un véhicule. 5
6. Procédé selon l'une quelconque des revendications précédentes **caractérisé en ce que** les systèmes de prises de vues fournissent des images numériques. 10
7. Procédé selon l'une quelconque des revendications **caractérisé en ce que** les procédés de codage et/ou décodage utilisent des techniques cryptographiques. 15
8. Procédé selon l'une quelconque des revendications précédentes, **caractérisé en ce que** les procédés de codage incorporent dans les données signatures, un sous-ensemble accessible et contenant l'ensemble des caractères alphanumériques suffisant pour représenter les données signatures. 20
25
9. Procédé selon l'une quelconque des revendications précédentes, **caractérisé en ce que** les systèmes d'exploitation appliquent aux données d'images prises, successivement un procédé de compression et le procédé de décompression associé, et mémorisent et/ou transfèrent les données obtenues vers des moyens de mémorisation et/ou de transmission. 30
10. Procédé selon l'une quelconque des revendications précédentes, **caractérisé en ce que** les premiers moyens de mémorisation et/ou de transmission et les seconds moyens de mémorisation et/ou de transmission sont confondus. 35
40
11. Procédé selon l'une quelconque des revendications précédentes, **caractérisé en ce que** la table de reconnaissance des caractères est élaborée par application d'un code programme de reconnaissance des caractères. 45
12. Procédé selon l'une quelconque des revendications 1 à 10 **caractérisé en ce que**, la table de reconnaissance des caractères est élaborée à partir des données signatures graphiques testées. 50

Patentansprüche

1. Verfahren zur Authentifizierung von Bildern und insbesondere von Bildern von Fahrzeugen, die bei einem Verkehrsdelikt aufgenommen werden, das die folgenden Schritte umfasst: 55

- Die Bildaufnahmesysteme (3) werden verteilt und so angeordnet, dass sie die Aufnahme von Bildern und die Erfassung der Identifikationselemente (101) von Verkehrssündern (100) ermöglichen, wobei die Aufnahmemittel repräsentative Bilder der Aufnahmen bereitstellen, die nachstehend Bilddaten (30) genannt werden,
- Es werden nachstehend als Informationssysteme (2) bezeichnete Mittel zur Erfassung der physischen Daten über das Verkehrsdelikt vorgesehen, die nachstehend als Verstoßdaten (20) bezeichnet werden,
- Es werden erste Mittel zum Speichern und/oder Übertragen (430A) der Bilddaten und der Verstoßdaten vorgesehen,
- Es werden Betriebssysteme (4) zur Verwendung der gespeicherten und/oder übertragenen Daten vorgesehen, und diese sind im Wesentlichen **dadurch gekennzeichnet, dass**

- a) die Betriebssysteme aus den Verstoßdaten und einer grafischen Darstellung der alphanumerischen Zeichen (410), aus denen diese Verstoßdaten bestehen, neue Daten berechnen, die Bilder darstellen, die grafische Verstoßdaten (11) genannt werden,
- b) die Betriebssysteme die Bilddaten (30) und die grafischen Verstoßdaten (11) verschmelzen, um einen neuen Datensatz zur Bilddarstellung zu erzielen, der grafische Identifizierungsdaten (12) genannt wird, wobei die Bilddaten (30) und die grafischen Verstoßdaten Teilgruppen dieses neuen Datensatzes (12) bilden, die für die Prozessoren der Betriebssysteme zugänglich sind,
- c) die Betriebssysteme einen nichtbijektiven Berechnungsprozess einsetzen, der auch als nichtbijektive f-Funktion bezeichnet wird, der auf die grafischen Identifizierungsdaten (12) angewendet wird und zu einem Datensatz führt, der im Folgenden als zusammengefasste Daten (31) bezeichnet wird, wobei die zusammengefassten Daten Sätze von 160 Bit Daten sind, die es nicht zulassen, zu den grafischen Identifizierungsdaten (12) zurückzukehren,
- d) die Betriebssysteme ein Codiervorgehen mit dem Code c auf die zusammengefassten Daten (31) anwenden, das ein zugehöriges Decodiervorgehen mit dem Code c^{-1} besitzt, um einen neuen Datensatz zu erzielen, der als codierte zusammengefasste Daten (32) bezeichnet wird,
- e) die Betriebssysteme die codierten zusammengefassten Daten (32) mit Alphabetdaten (420) verschmelzen, um einen Datensatz zu erzielen, der Signaturdaten

(33) genannt wird,
 f) die Betriebssysteme aus den Signaturdaten (33) und einer grafischen Darstellung der alphanumerischen Zeichen (410), die diese Signaturdaten (33) bilden, neue Bilddarstellungsdaten berechnen, die als grafische Signaturdaten (13) bezeichnet werden,
 g) die Betriebssysteme die grafischen Identifizierungsdaten (12) und die grafischen Signaturdaten (13) verschmelzen, um einen neuen Satz Bilddarstellungsdaten zu erzielen, wobei die grafischen Identifizierungsdaten und diese grafischen Signaturdaten zugängliche Teilgruppen dieses neuen Datensatzes bilden, die als grafische authentifizierbare Daten (14) bezeichnet werden, wobei die grafischen Signaturdaten aus einer Punktmatrix oder einem Barcode bestehen,
 h) zweite Mittel zum Speichern und/oder Übertragen (430B) der grafischen authentifizierbaren Daten (14) vorgesehen sind,
 i) Steuereinheiten (5) vorgesehen sind, die die in den zweiten Speicher- und/oder Übertragungsmitteln gespeicherten grafischen authentifizierbaren Daten jeweils lesen und/oder empfangen können, wobei die tatsächlich gelesenen und/oder empfangenen Daten als grafische empfangene Daten (50) bezeichnet werden,
 j) die Steuereinheiten unter den grafischen empfangenen Daten nach der Teilgruppe der grafischen Identifizierungsdaten suchen, die nachstehend als die getesteten grafischen Identifizierungsdaten (51) bezeichnet werden,
 k) die Steuereinheiten unter den grafischen empfangenen Daten die Teilgruppe der grafischen Signaturdaten suchen, die nachstehend als die getesteten grafischen Signaturdaten (52) bezeichnet werden,
 l) die Steuereinheiten unter den getesteten grafischen Signaturdaten und einer Erkennungstabelle (510) der alphanumerischen Zeichen nach einem Datensatz suchen, der die Signaturdaten darstellt, die als die getesteten Signaturdaten (53) bezeichnet werden,
 m) die Steuereinheiten mit Anwendung der nichtbijektiven f-Funktion auf die getesteten grafischen Identifizierungsdaten einen Datensatz berechnen, der getestete zusammengefasste Daten (55) genannt wird,
 n) die Steuereinheiten das c^{-1} Decodierverfahren auf die getesteten Signaturdaten anwenden, um einen Datensatz zu erzielen, der als empfangene zusammengefasste

Daten (54) bezeichnet wird, und
 o) die Steuereinheiten die empfangenen zusammengefassten Daten und die getesteten zusammengefassten Daten vergleichen und ein Alarmsignal anlegen, wenn diese Daten nicht identisch sind, oder ein Bestätigungssignal, wenn sie es sind.

2. Verfahren nach Anspruch 1, **dadurch gekennzeichnet, dass** die Betriebssysteme Folgendes auf die Bilddaten (30) anwenden:

- Entropische Datenkompressionsverfahren zur Reduzierung der Größe der zum Abspeichern der Bilddaten notwendigen Speicher und/oder der Kapazität der Übertragungsmittel dieser Daten und/oder
- jede andere Verarbeitung, wie z. B. Kontrastverstärkung zur Vereinfachung der Identifizierung des beschädigten Fahrzeugs,
- und dadurch, dass am Ende dieser Verarbeitungen die genannten Daten zur Bilddarstellung (30) als grafische Ausgangsdaten (10) bezeichnet werden.

3. Verfahren nach Anspruch 1 oder 2, **dadurch gekennzeichnet, dass** die Informationssysteme Mittel zum Messen der Geschwindigkeit von Fahrzeugen aufweisen.

4. Verfahren nach Anspruch 1 oder 2, **dadurch gekennzeichnet, dass** die Informationssysteme Mittel zum Erkennen des Vorhandenseins eines nicht autorisierten Fahrzeugs in einer reservierten Fahrspur beinhalten.

5. Verfahren nach Anspruch 1 oder 2, **dadurch gekennzeichnet, dass** die Informationssysteme Mittel zum Erkennen des Überfahrens einer roten Ampel durch ein Fahrzeug beinhalten.

6. Verfahren nach einem beliebigen der vorstehenden Ansprüche, **dadurch gekennzeichnet, dass** die Bildaufnahmesysteme digitale Bilder bereitstellen.

7. Verfahren nach einem beliebigen der vorstehenden Ansprüche, **dadurch gekennzeichnet, dass** die Codier- und/oder Decodierverfahren kryptographische Techniken verwenden.

8. Verfahren nach einem beliebigen der vorstehenden Ansprüche, **dadurch gekennzeichnet, dass** die Codierverfahren eine zugängliche Teilgruppe in die Signaturdaten aufnehmen, die alphanumerische Zeichen in ausreichender Menge enthalten, um die Signaturdaten darzustellen

9. Verfahren nach einem beliebigen der vorstehenden

Ansprüche, **dadurch gekennzeichnet, dass** die Betriebssysteme nacheinander ein Kompressionsverfahren und das zugehörige Dekompressionsverfahren auf die Bilddaten anwenden und die erzielten Daten speichern und/oder an Speicher- und/oder Übertragungsmittel übertragen. 5

10. Verfahren nach einem beliebigen der vorstehenden Ansprüche, **dadurch gekennzeichnet, dass** das erste Speicher- und/oder Übertragungsmittel und das zweite Speicher- und/oder Übertragungsmittel zusammenge- 10

11. Verfahren nach einem beliebigen der vorstehenden Ansprüche, **dadurch gekennzeichnet, dass** die Zeichenerkennungstabelle durch Anwendung eines Zeichenerkennungs-Programmcodes erarbeitet wird. 15

12. Verfahren nach einem beliebigen der vorstehenden Ansprüche 1 bis 10, **dadurch gekennzeichnet, dass** die Zeichenerkennungstabelle aus den getes- 20

Claims 25

1. A process for authentication of images and especially of images of offending vehicles comprising the following steps: 30

- photographic systems (3) are distributed, arranged so as to enable the taking of images and the input of identification elements (101) of offenders (100), the photographic means providing data representative of the taken images, hereinbelow called data of taken images (30), 35
- means are provided, hereinbelow called information systems (2), for inputting physical information relative to the infraction, hereinbelow called infraction data (20), 40
- first storage and/or transmission means (430A) of the data of taken images and the infraction data are provided,
- operating systems (4) are provided to exploit the stored and/or transmitted data, 45

and is essentially **characterized in that:**

- a) from the infraction data and a graphic representation of the alphanumeric characters (410) constituting these infraction data, the operating systems calculate new data representative of images, called graphic infraction data (11), 50
- b) the operating systems merge the data of taken images (30) and the graphic infraction data (11) so as to obtain a new set of data representative of images, called graphic identifying data 55

(12), in which the data of taken images (30) and the graphic infraction data constitute subsets accessible by processors constituting operating systems of this new set of data,

c) the operating systems execute a non-bijective calculation process, called non-bijective function noted f, applied to the identifying graphic data (12) and resulting in a set of data hereinbelow called summarized data (31), said summarized data being sets of 160 bits of information not relating back to the identifying graphic data (12),

d) the operating systems apply to the summarized data (31) a coding process noted c, having an associated decoding process noted c⁻¹, to obtain a new set of data, called summarized coded data (32),

e) the operating systems merge summarized coded data (32) with alphabet data (420) to obtain a new set of data, called signature data (33), f) the operating systems calculate, from the signature data (33) and a graphic representation of the alphanumeric characters (410) constituting these signature data (33) new data representative of images, called graphic signature data (13),

g) the operating systems merge the graphic identifying data (12) and the graphic signature data (13) so as to obtain a new set of data representative of images, in which the graphic identifying data and these graphic signature data constitute accessible subsets of this new set of data, called graphic authenticatable data (14), where the graphic signature data are constituted by a matrix of points or barcodes,

h) second storage and/or transmission means (430B) of graphic authenticatable data (14) are provided,

i) control units (5) are provided which can respectively read and/or receive the authenticatable graphic data stored in the second storage and/or transmission means, the data effectively read and/or received being called received graphic data (50),

j) the control units search among the received graphic data for the subset of identifying graphic data, hereinbelow called tested identifying graphic data (51),

k) the control units search among the received graphic data for the subset of graphic signature data, hereinbelow called tested graphic signature data (52),

l) the control units search for a set of data representative of signature data, called tested signature data (53), from the tested signature data graphic and a recognition table (510) of alphanumeric characters,

m) the control units calculate a set of data, called

- received tested summarized data (55) by application of the non-bijective function f to the tested identifying graphic data,
- n) the control units apply the decoding process c^{-1} to the tested signature data to obtain a set of data, called tested summarized data (54), and
- o) the control units compare the received summarized data and the tested summarized data, and supply an alert signal when these data are not identical and/or a confirmation signal when they are.
2. The process according to claim 1, **characterized in that** the operating systems apply to the data of taken images (30):
 - entropic compression processes of data for reducing the size of memories necessary for storing the data of taken images and/or the capacity of transmission means of these data, and/or
 - any other processing of contrast reinforcement type for making identification of the offending vehicle easier,
 - and **in that** on completion of these processing events said data (30) representative of images are called initial graphic images (10).
 3. The process according to claim 1 or 2, **characterized in that** the information systems comprise means for measuring the speed of vehicles.
 4. The process according to claim 1 or 2, **characterized in that** the information systems comprise means for detecting the presence of a non-authorized vehicle in a reserved lane.
 5. The process according to claim 1 or 2, **characterized in that** the information systems comprise means for detecting when a vehicle travels through a red light.
 6. The process according to any one of the preceding claims **characterized in that** photographic systems provide digital images.
 7. The process according to any one of the preceding claims, **characterized in that** coding and/or decoding processes utilize cryptographic techniques.
 8. The process according to any one of the preceding claims, **characterized in that** coding processes incorporate an accessible subset containing all alphanumeric characters sufficient to represent the signature data into the signature data.
 9. The process according to any one of the preceding claims, **characterized in that** operating systems successively apply a compression process and the associated decompression process to the image data taken, and store and/or transfer the obtained data to storage and/or transmission means.
 10. The process according to any one of the preceding claims, **characterized in that** the first storage and/or transmission means and the second storage and/or transmission means are combined.
 11. The process according to any one of the preceding claims, **characterized in that** the character recognition table is developed by application of a character recognition code programme.
 12. The process according to any one of claims 1 to 10, **characterized in that** the character recognition table is developed from the tested graphic signature data.

Figure 1 :

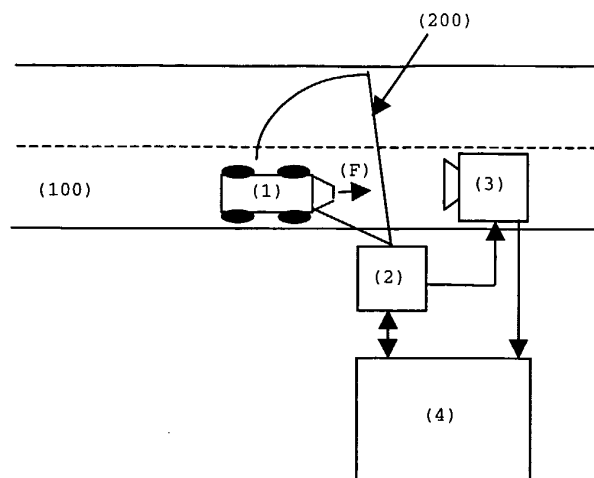


Figure 2 :

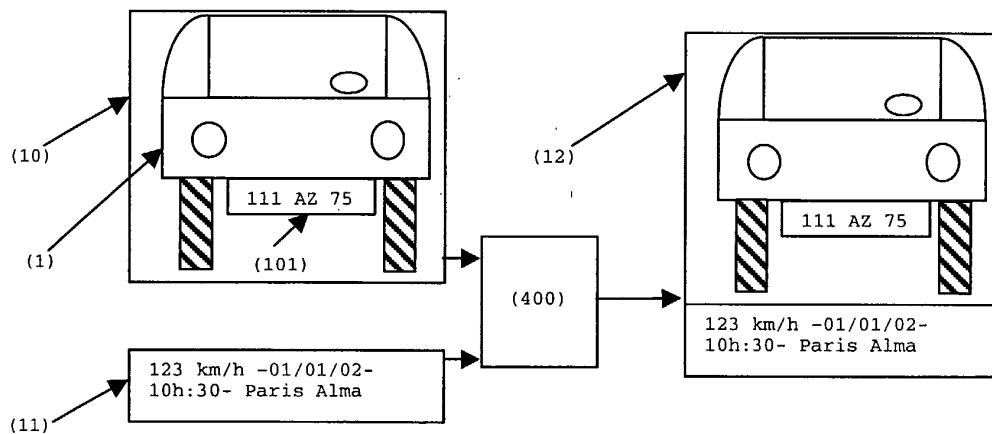


Figure 3 :

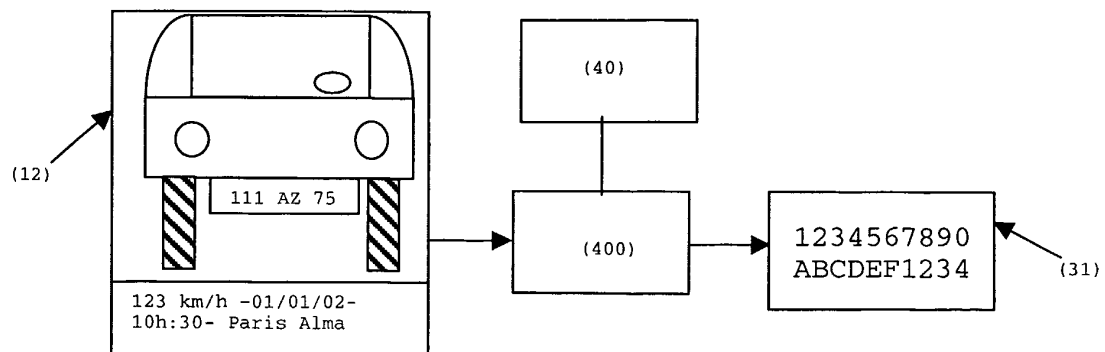


Figure 4 :

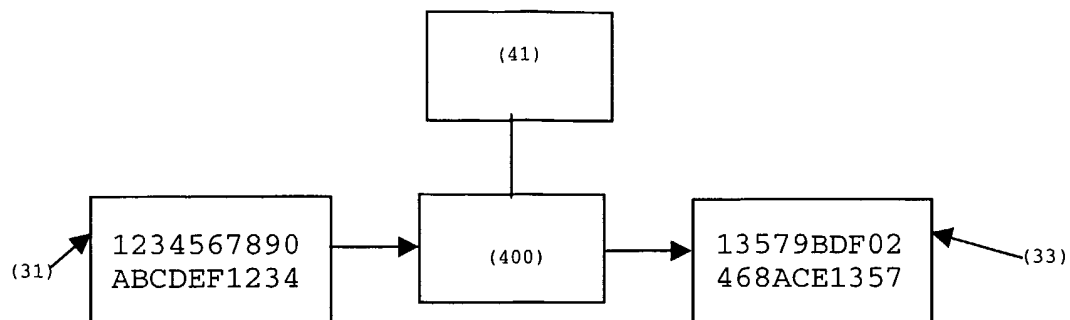


Figure 5 :

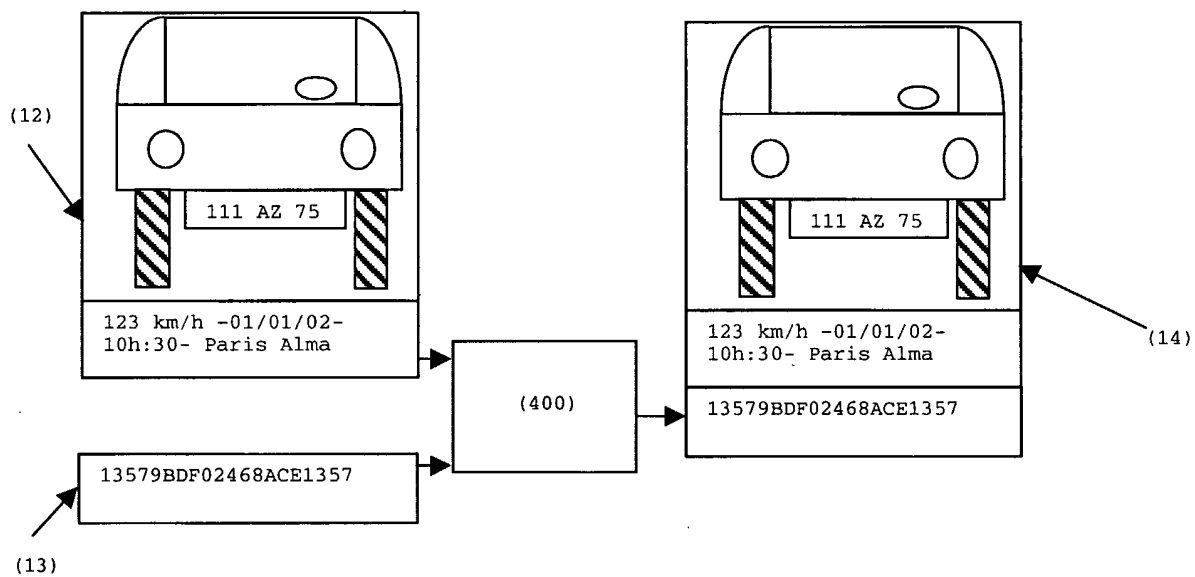
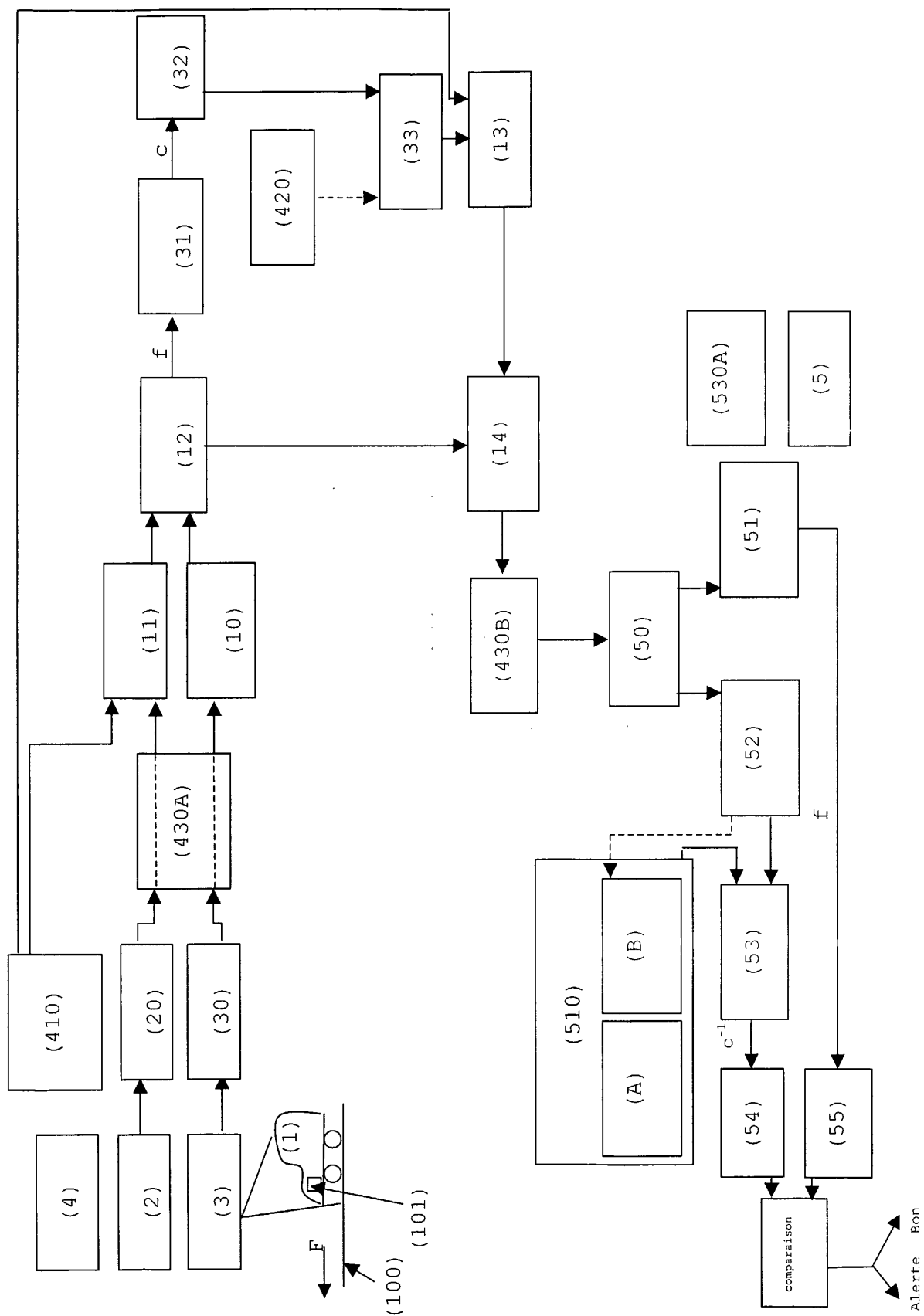


Figure 6



RÉFÉRENCES CITÉES DANS LA DESCRIPTION

Cette liste de références citées par le demandeur vise uniquement à aider le lecteur et ne fait pas partie du document de brevet européen. Même si le plus grand soin a été accordé à sa conception, des erreurs ou des omissions ne peuvent être exclues et l'OEB décline toute responsabilité à cet égard.

Documents brevets cités dans la description

- US 5381155 A [0011]
- EP 0621572 A [0019]
- WO 0208400 A [0019]
- US 5563590 A [0023]
- US 6269446 B [0033]
- US 4405829 A [0075]