



(12) **EUROPEAN PATENT APPLICATION**

(43) Date of publication:
11.04.2018 Bulletin 2018/15

(51) Int Cl.:
G08G 1/01 (2006.01) G08G 1/017 (2006.01)

(21) Application number: **16192155.6**

(22) Date of filing: **04.10.2016**

(84) Designated Contracting States:
AL AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HR HU IE IS IT LI LT LU LV MC MK MT NL NO PL PT RO RS SE SI SK SM TR
Designated Extension States:
BA ME
Designated Validation States:
MA MD

(72) Inventors:
• **Meier, Beat**
6300 Zug (CH)
• **Krpoun, Laurence**
8703 Erlenbach (CH)

(74) Representative: **Karl, Christof**
Bardehle Pagenberg Partnerschaft mbB
Patentanwälte, Rechtsanwälte
Prinzregentenplatz 7
81675 München (DE)

(60) Divisional application:
17177232.0 / 3 306 587

(71) Applicant: **FAST Recognition AG**
6300 Zug (CH)

(54) **IDENTIFICATION OF A MOBILE DEVICE USED BY THE USER OF A VEHICLE**

(57) A method and system for identifying mobile communication devices used together with vehicles, or vehicles used together with mobile communication devices, are provided. The method comprises obtaining, for each of one or more vehicles, one or more vehicle identification data sets, each comprising a vehicle identifier and a vehicle identifier acquisition site, the vehicle identifier acquisition site comprising a time and a location at which the vehicle identifier has been acquired; obtaining, for each of one or more mobile communication devices, one or more mobile communication device identification data sets, each comprising a mobile communication device identifier and a mobile communication device identifier acquisition site, the mobile communication device identifier acquisition site comprising a time and a location at which the mobile communication device identifier has been acquired; generating a vehicle and mobile communication device association set, wherein each entry of the association set associates a vehicle identification data set and a mobile communication device identification data set and the vehicle identifier acquisition site comprised in the vehicle identification data set corresponds to the mobile communication device identifier acquisition site comprised in the associated mobile communication device identification data set; and based on the generated association set, identifying at least one mobile communication device used together with a specified vehicle, or at least one vehicle used together with a specified mobile communication device.

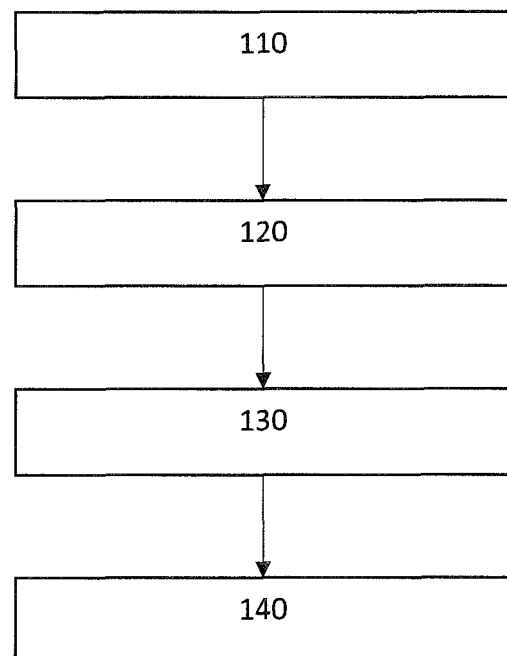


Fig. 1

Description

BACKGROUND OF THE INVENTION

5 Field of the invention

[0001] The present invention relates to a method and system for identifying mobile communication devices used together with vehicles, or vehicles used together with mobile communication devices.

10 Description of Prior Art

[0002] Automatic number plate recognition, ANPR, also known as Automatic License Plate recognition, ALPR, allows to gather information on vehicles in road traffic, using optical character recognition on images of the vehicles' license plates. The images of license plates can be captured by cameras specifically designed for ANPR. ANPR cameras are mounted on top of a road or next to a road and capture images of vehicles passing through. The images are then analyzed resulting in a set of data called meta-data extracted from each captured license plate.

[0003] It is known that data comprising the information gathered with ANPR can be stored, e.g. in a database hosted by a computer server, for further use by authorized entities, e.g. for law enforcement and security.

[0004] Another domain of research and technology is radio frequency and mobile communication. A mobile communication device, e.g. a user equipment, UE, is identified by a unique identification, the International Mobile Equipment Identity. Further, a user of a UE is identified by another unique identification, the International Mobile Subscriber Identity, or IMSI, which identifies the user in a mobile communication network of a mobile communication provider. It is further known that one or both identifications can be captured by a cellular identification (CID) device, which implements functionality of a base transceiver station, BTS. That is, a CID device can identify the above mentioned unique identification of a nearby UE and/or its user. The data captured by a CID device can also be stored, e.g. in a database hosted by a computer server.

[0005] Currently, there is however no system that identifies an individual using both, a vehicle and a mobile communication device. Thus, methods and systems for identifying mobile communication devices used together with vehicles, or vehicles used together with mobile communication devices in an efficient manner are highly desirable. It is also desirable that such methods and systems handle the sensitive data about identification of UE in a secure manner, preferably such that even the service provider operating the data base where the data is stored cannot access the data, but only an authorized agency, e.g. law enforcement agency.

SUMMARY OF THE INVENTION

35 **[0006]** Some or all of these objects are achieved by the subject matter of the independent claims. Preferred embodiments are subject of the dependent claims.

[0007] A 1st embodiment of the invention is a method for identifying mobile communication devices used together with vehicles, or vehicles used together with mobile communication devices, the method comprising the steps of:

40 obtaining, for each of one or more vehicles, one or more vehicle identification data sets, each comprising a vehicle identifier and a vehicle identifier acquisition site, the vehicle identifier acquisition site comprising a time and a location at which the vehicle identifier has been acquired;
 obtaining, for each of one or more mobile communication devices, one or more mobile communication device identification data sets, each comprising a mobile communication device identifier and a mobile communication device identifier acquisition site, the mobile communication device identifier acquisition site comprising a time and a location at which the mobile communication device identifier has been acquired;
 45 generating a vehicle and mobile communication device association set, wherein each entry of the association set associates a vehicle identification data set and a mobile communication device identification data set and the vehicle identifier acquisition site comprised in the vehicle identification data set corresponds to the mobile communication device identifier acquisition site comprised in the associated mobile communication device identification data set; and
 based on the generated association set, identifying at least one mobile communication device used together with a specified vehicle, or at least one vehicle used together with a specified mobile communication device.

55 **[0008]** According to a 2nd embodiment, in the 1st embodiment, a vehicle identifier acquisition site corresponds to a mobile communication device identifier acquisition site if:

the location comprised in the vehicle identifier acquisition site corresponds to the location comprised in the mobile

communication device identifier acquisition site; and
the time comprised in the vehicle identifier acquisition site corresponds to the time comprised in the mobile communication device identifier acquisition site.

[0009] According to a 3rd embodiment, in the 2nd embodiment, the time comprised in a vehicle identifier acquisition site corresponds to the time comprised in a mobile communication device identifier acquisition site if the time comprised in the vehicle identifier acquisition site and the time comprised in the mobile communication device identifier acquisition site are within the same predefined time interval.

[0010] According to a 4th embodiment, in any one of the preceding embodiments, the method comprises further:

acquiring a user input specifying a vehicle identifier;
determining a vehicle identifier associated set of preferably all mobile communication device identifiers comprised in the mobile communication device identification data sets associated in the associated set with vehicle identification data sets comprising the specified vehicle identifier; and
for each of the mobile communication device identifiers comprised in the vehicle identifier associated set, calculating a confidence score for an association of the specified vehicle identifier with the mobile communication device identifier indicating a likelihood that the vehicle identified by the specified vehicle identifier has correctly been associated with a mobile communication device identified by the mobile communication device identifier.

[0011] According to a 5th embodiment, in the 4th embodiment, calculating the confidence score for the association of the specified vehicle identifier with a mobile communication device identifier comprises:

determining, in the association set, a first number A, specifying a number of entries associating a vehicle identification data set comprising the specified vehicle identifier with a mobile communication device identification data set comprising the mobile communication device identifier;
determining a first ratio of the first number A and a second number |Tp|, specifying a number of vehicle identification data sets comprising the specified vehicle identifier;
determining a second ratio of the first number A and a third numbers |Dcid|, specifying a number of mobile communication device identification data sets comprising the mobile communication device identifier; and
determining the sum of the first ratio and the second ratio.

[0012] According to a 6th embodiment, in any one of the 1st to 3rd embodiments, the method comprises further:

acquiring a user input specifying a mobile communication device identifier;
determining a mobile communication device identifier associated set of preferably all vehicle identifiers comprised in the vehicle identification data sets associated in the associated set with mobile communication device identification data sets comprising the specified mobile communication device identifier; and
for each of the vehicle identifiers comprised in the mobile communication device identifier associated set, calculating a confidence score for an association of the specified mobile communication device identifier with the vehicle identifier indicating a likelihood that the mobile communication device identified by the specified mobile communication device identifier has correctly been associated with a vehicle identified by the vehicle identifier.

[0013] According to a 7th embodiment, in the 6th embodiment, calculating the confidence score for the association of the specified mobile communication device identifier with a vehicle identifier comprises:

determining, in the association set, a first number A, specifying a number of entries associating a vehicle identification data set comprising the vehicle identifier with a mobile communication device identification data set comprising the specified mobile communication device identifier;
determining a first ratio of the first number A and a second number |Tp|, specifying a number of vehicle identification data sets comprising the vehicle identifier;
determining a second ratio of the first number A and a third number |Dcid| specifying a number of mobile communication device identification data sets comprising the specified mobile communication device identifier; and
determining the sum of the first ratio and the second ratio.

[0014] According to an 8th embodiment, in the 5th or 7th embodiment, respectively, calculating the confidence score comprises multiplying the sum with a factor, preferably 0.5.

[0015] According to a 9th embodiment, in any one of the preceding embodiments, the method comprises further the steps of

acquiring, for each of the one or more vehicles, the one or more vehicle identification data sets, and/or
acquiring, for each of one or more mobile communication devices, one or more mobile communication device
identification data sets.

5 **[0016]** A 10th embodiment of the invention is a method for acquiring, in a secured manner, a mobile communication
device identification data set, the method comprising the steps of:

acquiring, for each of one or more mobile communication devices, a mobile communication device identifier;
generating a first encrypted mobile communication device identifier by encrypting the mobile communication device
10 identifier with a first encryption method, wherein the first encryption method uses a public key for encryption and
requires a paired private key for decryption; and
transmitting, to a server, a mobile communication device identification data set comprising the first encrypted mobile
communication device identifier.

15 **[0017]** According to an 11th embodiment, in the 10th embodiment,

the step of generating the first encrypted mobile communication device identifier further comprises generating a
second encrypted mobile communication device identifier by encrypting the mobile communication device identifier
with a second encryption method, wherein the second encryption method uses a one-way mapping function such
20 that a second encrypted mobile communication device identifier cannot be decrypted; and
the mobile communication device identification data set transmitted in the transmitting step comprises the first and
second encrypted mobile communication device identifiers.

25 **[0018]** A 12th embodiment of the invention is a method for handling, in a secured manner, information regarding mobile
communication devices used together with vehicles, and/or regarding vehicles used together with mobile communication
devices, the method comprising the steps of:

storing, for each of one or more vehicles, one or more vehicle identification data sets, each comprising a vehicle
identifier;
30 storing, for each of one or more mobile communication devices, one or more mobile communication device identi-
fication data sets, each comprising a first and a second encrypted mobile communication device identifier generated
with a first and a second encryption method, wherein the first encryption method uses a public key for encryption
and requires a paired private key for decryption, and wherein the second encryption method uses a one-way mapping
function such that the second encrypted mobile communication device identifier cannot be decrypted.

35 **[0019]** According to a 13th embodiment, in the 12th embodiment, the method further comprises the steps of

acquiring a user input specifying a vehicle identifier;
identifying at least one mobile communication device used together with a vehicle identified by the specified vehicle
40 identifier by means of the mobile communication device identification data sets and the vehicle identification data
sets; and
outputting, for the identified at least one mobile communication device, the first and/or second encrypted mobile
communication device identifier comprised in the mobile communication device identification data set of the identified
at least one mobile communication device.

45 **[0020]** According to a 14th embodiment, in the 13th embodiment, the at least one mobile communication device used
together with the vehicle identified by the specified vehicle identifier is identified in accordance with the method of any
one of the 1st to 5th embodiment, or the 8th embodiment.

50 **[0021]** According to a 15th embodiment, in any one of the 10th to 14th embodiment, the method comprises further the
steps of

acquiring a user input specifying a mobile communication device identifier;
if the mobile communication device identifier is not encrypted with the second encryption method, encrypting the
specified mobile communication device identifier using the second encryption method;
55 identifying at least one vehicle used together with the mobile communication device identified by the specified mobile
communication device identifier by means of the second encrypted mobile communication device identifiers com-
prised in the mobile communication device identification data sets and the vehicle identification data sets; and
outputting the vehicle identifier of the identified at least one vehicle.

[0022] According to a 16th embodiment, in the 15th embodiment, the at least one vehicle used together with the mobile communication device identified by the specified mobile communication device identifier is identified in accordance with the method of any one of claim 1 to 3, or any one of claims 6 to 8.

[0023] According to a 17th embodiment, in any one of the 12th to 16th embodiments, the

method comprises further the step of
receiving the one or more vehicle identification data sets from an apparatus for providing, in a secured manner, information regarding mobile communication devices.

[0024] According to an 18th embodiment, in any one of the 12th to 17th embodiments, the method comprises further the steps of the 9th embodiment.

[0025] According to a 19th embodiment, in any one of the 12th to 18th embodiments, the method comprises further the steps of acquiring, for each of the one or more vehicles, the one or more vehicle identification data sets.

[0026] According to a 20th embodiment, in any one of the 10th to 19th embodiments, a mobile communication device identification data set does not comprise an unencrypted mobile communication device identifier of the respective mobile communication device.

[0027] According to a 21st embodiment, in any one of the 10th to 20th embodiments, the second encryption method is a hash encryption.

[0028] According to a 22nd embodiment, in any one of the 9th or 19th embodiments, or the 20th and 21st embodiments, when depending from the 19th embodiment, acquiring a vehicle identification data set for a vehicle comprises:

capturing an image of the vehicle with a camera; and
processing the captured image with image processing to extract license plate data associated with a license plate of the vehicle.

[0029] According to a 23rd embodiment, in the 22nd embodiment, the camera is configured for Automatic Number Plate recognition, ANPR, or for Automatic License Plate recognition, ALPR.

[0030] According to a 24th embodiment, in any one of the 22nd or 23rd embodiments, acquiring a vehicle identification data set for one of the plurality of vehicles further comprises:

querying a vehicle identification server with the extracted license plate data; and
in response, receiving, from the vehicle identification server, the vehicle identifier identifying the vehicle.

[0031] According to a 25th embodiment, in any one of the 9th, 10th, or any one of the 18th to 24th embodiments, when depending from the 9th embodiment, acquiring a mobile communication device identification data set for a mobile communication device comprises capturing at least one identification of the mobile communication device by a capturing device, preferably one of a base station operating according to a standard for wireless communication.

[0032] According to a 26th embodiment, in the 25th embodiment, an identification of the mobile communication device captured by the capturing device is:

an identifier associated with a subscriber module comprised by the mobile communication device; or
an identifier associated with the mobile communication device.

[0033] According to a 27th embodiment, in any of the 25th or 26th embodiments, acquiring a mobile communication device identification data set for a mobile communication device further comprises:

querying a mobile communication device identification server with at least one of the captured identifications; and
in response, receiving, from the mobile communication device identification server, the mobile communication device identifier identifying the mobile communication device.

[0034] A 28th embodiment of the invention is a system for identifying mobile communication devices used together with vehicles, or vehicles used together with mobile communication devices, the system comprising means configured for carrying out the steps of the method of any one of the 1st to 9th embodiments, or any one of the 22nd to 27th embodiments, when depending from the 1st embodiment.

[0035] A 29th embodiment of the invention is an apparatus for acquiring, in a secured manner, a mobile communication device identification data set, the apparatus comprising means configured for carrying out the steps of the method according to the 10th embodiment, or any one of the 20th or 21st embodiments, when dependent from the 10th embodiment, or any one of the 25th to 27th embodiments when depending from the 10th embodiment.

[0036] A 30th embodiment of the invention is a server for handling, in a secured manner, information regarding mobile communication devices which are used together with vehicles, or regarding vehicles used together with mobile communication devices, the server comprising means configured for carrying out the steps of the method of any one of the 12th to 19th embodiments, or any one of the 20th or 21st embodiments, when dependent from the 11th embodiment.

[0037] A 31st embodiment of the invention is a system for identifying, in a secured manner, mobile communication devices used together with vehicles, or vehicles used together with mobile communication devices, the system comprising one or more apparatus according to the 29th embodiment and one or more servers according to the 30th embodiment, and optionally one or more apparatus comprising means configured for carrying out the steps of the method mentioned in any one of the 22nd to 24th embodiments, or a combination thereof.

[0038] It is to be understood that both the foregoing general description and the following detailed description are exemplary, and are intended to provide further explanation of the invention as claimed. Other advantages and features of the invention will be apparent from the following description, drawings and claims.

BRIEF DESCRIPTION OF THE DRAWINGS

[0039] The features of the invention are set forth with particularity in the appended claims. The invention may be best understood by reference to the following detailed description of the invention, which describes an exemplary embodiment of the invention, taken in conjunction with the accompanying drawings, in which:

Fig. 1 is a flowchart showing the steps of a method according to an embodiment of the present invention;

Fig. 2 is a flowchart showing further steps of the method of Fig. 1 according to some embodiments of the present invention;

Fig. 3 is a flowchart showing further steps of the method of Fig. 2 according to some embodiments of the present invention;

Fig. 4 is a flowchart showing further steps of the method of Fig. 1 according to some preferable embodiments of the present invention;

Fig. 5 is a flowchart showing further steps of the method of Fig. 4 according to some embodiments of the present invention;

Fig. 6 is a flowchart showing steps of a method according to some further embodiments of the present invention;

Fig. 7 is a flowchart showing steps of a method according to some further embodiments of the present invention;

Fig. 8 is a schematic view of a system for carrying out the methods according to some further embodiments of the present invention; and

Fig. 9 is an alternative view of the system of Fig. 8.

Fig. 10 is another alternative view of the system of Fig. 8.

DETAILED DESCRIPTION OF THE INVENTION

[0040] In cooperation with the attached drawings, the technical contents and detailed description of the present invention are described hereinafter according to preferred embodiments.

[0041] Reference is made to Fig. 1 which is a flowchart showing the steps of a method according to an embodiment of the present invention. The method shown in Fig. 1 is for identifying mobile communication devices used together with vehicles, or vehicles used together with mobile communication devices.

[0042] In a step 110, for each of one or more vehicles, one or more vehicle identification data sets are obtained, e.g. acquired by a camera which is configured for Automatic Number Plate recognition, ANPR (also referred to as Automatic License Plate recognition, ALPR). The ANPR camera captures an image of the vehicle. The captured image is processed with image processing to extract license plate data associated with a license plate of the vehicle, e.g. the plate number. The extracted license plate data can then be used to query a vehicle identification server, to receive a vehicle identifier which identifies the vehicle.

[0043] A vehicle identification data set obtained for a vehicle comprises the vehicle identifier, and further a vehicle

identifier acquisition site. The vehicle identifier acquisition site is used to store time and location at which the vehicle identifier has been acquired, e.g. captured by the respective ANPR camera. A vehicle identification data set is also referred to as a transit. There is usually more than one transit per plate number. This corresponds to a vehicle being recorded at different locations in a city.

[0044] In another step 120, for each of one or more mobile communication devices, one or more mobile communication device identification data sets are obtained, e.g. acquired by capturing at least one identification of the mobile communication device by a capturing device. The capturing device is preferably a base station operating according to a standard for wireless communication, also referred to as a CID device as discussed above. In this context, an identification of the mobile communication device captured by the capturing device is e.g. an identifier associated with a subscriber module comprised by the mobile communication device (preferably an International Mobile Subscriber Identity, or IMSI), or an identifier associated with the mobile communication device (preferably an International Mobile Station Equipment Identity, or IMEI). The captured identifications can be used to query a mobile communication device identification server, to receive information about the user of the identified device.

[0045] A mobile communication device identification data set obtained for a mobile communication device comprises the mobile communication device identifier and further a mobile communication device identifier acquisition site. The mobile communication device identifier acquisition site is used to store time and location at which the mobile communication device identifier has been acquired, e.g. captured by the respective base station.

[0046] Subsequent to these obtaining steps 110, 120, a vehicle and mobile communication device association set is generated in step 130. Each entry of the association set associates a vehicle identification data set and a mobile communication device identification data set. The vehicle identifier acquisition site comprised in the vehicle identification data set corresponds to the mobile communication device identifier acquisition site comprised in the associated mobile communication device identification data set.

[0047] In other words, the obtained data sets for vehicles and mobile communication devices are combined, based on their acquisition time and location. In particular, a vehicle identifier acquisition site is determined to correspond to a mobile communication device identifier acquisition site if the location comprised in the vehicle identifier acquisition site corresponds to the location comprised in the mobile communication device identifier acquisition site, and the time comprised in the vehicle identifier acquisition site corresponds to the time comprised in the mobile communication device identifier acquisition site.

[0048] Preferably, the time comprised in a vehicle identifier acquisition site is determined to correspond to the time comprised in a mobile communication device identifier acquisition site if the time comprised in the vehicle identifier acquisition site and the time comprised in the mobile communication device identifier acquisition site are within the same predefined time interval. A preferably time interval is a time interval of five seconds, however other time intervals are also possible.

[0049] Fig. 9 shows an example of an acquisition site. An acquisition site preferably comprises one CID device 810 and one or more ANPR cameras 830, preferably one ANPR camera per road lane. While the CID device and the ANPR cameras deployed at a specific acquisition site can have slightly different GPS coordinates, each acquisition site is identified by a unique site identifier, e.g. a name or descriptor, represented by the location comprised in the vehicle identifier acquisition site and the mobile communication device identifier acquisition site. Accordingly, the CID device and the ANPR cameras deployed at a specific acquisition site are associated with the respective unique site identifier, stored as location. Consequently, the location comprised in a vehicle identifier acquisition site is determined to correspond to the location comprised in a mobile communication device identifier acquisition site if they are similar. As another option, the location of an acquisition site can be stored as GPS coordinates, and a range can be defined for slightly different GPS coordinates to be similar, thus defining the location of a specific acquisition site.

[0050] Based on the generated association set, at least one mobile communication device which is used together with a specified vehicle is identified in step 140. Alternatively, at least one vehicle which is used together with a specified mobile communication device is identified in step 140.

[0051] Fig. 2 is a flowchart showing further steps of the method of Fig. 1, according to a preferred embodiment of the present invention. In particular, a vehicle can be specified by a user of a system implementing the method. Thus, in step 210, a user input specifying a vehicle identifier is acquired. Then, in step 220, a vehicle identifier associated set is determined. The vehicle identifier associated set preferably comprises all mobile communication device identifiers which are comprised in the mobile communication device identification data sets, which have been associated previously, in the associated set, with vehicle identification data sets comprising the specified vehicle identifier.

[0052] In step 230, confidence scores are calculated for the determined associations between the specified vehicle and previously captured mobile communication devices. In particular, for each of the mobile communication device identifiers comprised in the vehicle identifier associated set, a confidence score for an association of the specified vehicle identifier with the mobile communication device identifier is calculated. The confidence score indicates a likelihood that the vehicle identified by the specified vehicle identifier has correctly been associated with the mobile communication device identified by the mobile communication device identifier.

[0053] Fig. 3 is a flowchart showing the sub-steps of step 230 of the method of Fig. 2 according to a preferred embodiment of the present invention.

[0054] In particular, as shown in Fig. 3, the step 230 of calculating the confidence score for an association of a specified vehicle identifier with a mobile communication device identifier comprises a step 230-1 of determining, in the association set, a first number $A(p, cid)$, which specifies a number of entries associating a vehicle identification data set comprising the specified vehicle identifier p with a mobile communication device identification data set comprising the mobile communication device identifier cid . In step 230-2, a first ratio of the first number $A(p, cid)$ and a second number $|Tp|$ is determined. $|Tp|$ specifies a number of vehicle identification data sets comprising the specified vehicle identifier p . In step 230-3, a second ratio of the first number $A(p, cid)$ and a third number $|Dcid|$ is determined. Here, $|Dcid|$ specifies a number of mobile communication device identification data sets comprising the mobile communication device identifier cid . Then, in step 230-4, the sum of the first ratio and the second ratio is determined, and the sum is preferably multiplied with a factor of 0.5.

[0055] In other words, let

- p be a vehicle identifier, e.g. a plate number,
- Tp be a set of associations, or transits, determined for a plate p and the number $|Tp|$ of vehicle identification data sets comprising the specified vehicle identifier p ,
- cid be a mobile communication device identifier, and
- $|Dcid|$ specify a number of mobile communication device identification data sets comprising the mobile communication device identifier cid .

[0056] Let us consider $a(p, cid)$ representing the number of associations between a plate number p and a mobile communication device identifier cid . It is noted that $a(p, cid)$ is determined as discussed above, by combining two obtained data sets regarding vehicles and mobile communication devices, based on the respective acquisition time and location. As discussed above, a plate p is associated to a cid if they were captured in the same time interval at the same site, with a site being a single location where road traffic and mobile phones presence are monitored. A plate p and a cid should be seen together many times for the associations to be likely.

[0057] Let further $A(p, cid)$ be the set of associations between p and cid , and $|A(p, cid)|$ the number of entries in the set. The confidence score for an association of a specified vehicle identifier, or plate, p and a mobile communication device identifier, or cid , is then computed as follows:

$$\text{score}(p, cid) = \frac{1}{2} * \left(\frac{|A(p, cid)|}{|Tp|} + \frac{|A(p, cid)|}{|Dcid|} \right)$$

[0058] The resulting confidence score is always in between 0 and 1. A score of 0 indicates that a mobile communication device identifier cid was never associated with the plate p . On the other hand, a score of 1 indicates that the cid was always associated with the plate p .

[0059] The search will return a score of 1 in the case that there are for example five transits with the plate number p , and every one of these transits is associated with the same cid . At the same time this specific cid will also appear exactly five times in the specified search parameters and every time will be associated with the specified plate number p . As discussed above, "associated" means that they were captured at the same site at about the same time. It should be noted that this does not mean that the transit will not be associated with other cid , and that the cid will not be associated with other plate numbers outside the search parameters.

[0060] Accordingly, the steps of the method as shown in Figs. 1 to 3 allow a user to search for mobile communication devices that are associated with a vehicle specified by the user. The method can however also be used for searching vehicles that are associated with a mobile communication device identified by the user.

[0061] Fig. 4 is a flowchart showing further steps of the method of Fig. 1 according to a preferred embodiment of the present invention. In particular, a mobile communication device can be specified by the user. Thus, in step 410, a user input specifying a mobile communication device identifier is acquired. Then, in step 420, a mobile communication device identifier associated set is determined. The mobile communication device identifier associated set preferably comprises all vehicle identifiers which are comprised in the vehicle identification data sets, which previously have been associated, in the associated set, with mobile communication device identification data sets comprising the specified mobile communication device identifier.

[0062] In step 430, similar to the method shown in Fig. 2 and discussed above, confidence scores are calculated, this time for the determined associations between the specified mobile communication device and previously captured vehicles. In particular, for each of the vehicle identifiers comprised in the mobile communication device identifier associated set, a confidence score for an association of the specified mobile communication device identifier with the vehicle

identifier is calculated. The confidence score again indicates a likelihood that the mobile communication device identified by the specified mobile communication device identifier has correctly been associated with a vehicle identified by the vehicle identifier.

[0063] Fig. 5 is a flowchart showing the sub-steps of step 430 of the method of Fig. 4 according to a preferred embodiment of the present invention.

[0064] As shown in Fig. 5, the step 430 of calculating the confidence score for an association of a specified mobile communication device identifier with a vehicle identifier comprises a step 430-1 of determining, in the association set, a first number $A(p, cid)$, which again specifies a number of entries associating a vehicle identification data set comprising the vehicle identifier p with a mobile communication device identification data set comprising the specified mobile communication device identifier cid . In step 430-2, again a first ratio of the first number $A(p, cid)$ and a second number $|Tp|$ is determined, and $|Tp|$ again specifies a number of vehicle identification data sets comprising the vehicle identifier p . In step 430-3, again a second ratio of the first number $A(p, cid)$ and a third number $|Dcid|$ is determined, wherein $|Dcid|$ specifies a number of mobile communication device identification data sets comprising the specified mobile communication device identifier cid . As above, finally in step 430-4, the sum of the first ratio and the second ratio is determined, and the sum is preferably multiplied with a factor of 0.5.

[0065] Thus, it is possible that a user searches for vehicle identifiers, e.g. plate numbers, that are associated with a mobile communication device specified by the user. The search is similar to the above as shown in Figs. 2 and 3. The confidence score is calculated in the same way as for the search with a plate number p , using the same formula as above:

$$score(p, cid) = \frac{1}{2} * \left(\frac{|A(p, cid)|}{|Tp|} + \frac{|A(p, cid)|}{|Dcid|} \right)$$

[0066] It should be noted that the calculated score is the same for both searches, but because the search is done differently (looking for all $cids$ captured together with a given plate p versus looking for all plates p captured together with a given cid), the result may be slightly different, e.g. due to point where the time intervals used for capturing are centered.

[0067] As a result of the above described methods, the present invention allows to combine the advances in the field of video surveillance and license plate recognition with new trends in mobile communications to associate traffic data to mobile data. The present invention thus leverages both technologies to collect information about traffic, namely license plates meta-data, time, and location information with mobile phone meta-data such as cellular and hardware identification, frequency, operator information, time, and location. The proposed methods use the data collected independently from both systems, namely ANPR cameras and CID devices, and merge them based on common information such as location and time. The invention involves making a statistical analysis on the merged data to provide statistically significant associations of traffic and mobile phones. This results in the possibility to track mobile communication devices, e.g. mobile phones, used with or in vehicles, e.g. cars, in an advantageous and efficient way.

[0068] Due to the sensitive nature of the data handled by the present invention, some embodiments relate to security measures to protect the data and the results of the proposed algorithms from unauthorized use. In particular, the above discussed IMSI and IMEI numbers can be used to track individuals, and therefore this information should be accessible only by authorized persons, e.g. authorized agencies.

[0069] Fig. 6 is a flowchart showing steps of a method according to a further embodiment of the present invention. The method of Fig. 6 is for acquiring a mobile communication device identification data set in a secured manner. In step 610, a mobile communication device identifier is acquired for each of one or more mobile communication devices. This is preferably done by a capturing device as discussed above, i.e. by a base station operating according to a standard for wireless communication, also referred to as a CID device.

[0070] In step 620, a first encrypted mobile communication device identifier is generated by encrypting the mobile communication device identifier with a first encryption method. The first encryption method uses a public key for encryption and further requires a paired private key for decryption. An example for the first encryption method is RSA (for Rivest-Shamir-Adleman), which is an asymmetric encryption method that can be used for secure data transmission. "Asymmetric" here means that the key used for encryption is public and differs from the decryption key which is kept secret. Preferably, RSA is used with a 1024-bit encryption key.

[0071] In step 630, a mobile communication device identification data set comprising the first encrypted mobile communication device identifier is transmitted to a server.

[0072] The method of Fig. 6 is preferably executed by a CID device as discussed above.

[0073] In some embodiments, step 620 of generating the first encrypted mobile communication device identifier further comprises generating a second encrypted mobile communication device identifier by encrypting the mobile communication device identifier with a second encryption method. The second encryption method uses a one-way mapping function such that a second encrypted mobile communication device identifier cannot be decrypted. Accordingly, in

these embodiments the mobile communication device identification data set transmitted in the transmitting step 630 comprises the first and second encrypted mobile communication device identifiers.

[0074] In further embodiments, the steps of the method of Fig. 6 are performed batch-wise. That is, the CID device performs the steps of the method in certain time intervals, e.g. every five seconds. The time interval is a parameter, and other time intervals are possible. In each time interval, a plurality of mobile communication device identifiers are acquired in step 610. Then, each of the acquired plurality of mobile communication device identifiers are encrypted (either only using RSA, or using both, RSA and SHA) in step 620. Finally, a corresponding plurality of mobile communication device identification data sets is transmitted to the centralized server in step 630.

[0075] The advantage of the batch-wise performing of the method of Fig. 6 is that the CID device only needs to set up a connection to the centralized server once, to transmit a plurality of mobile communication device identification data sets in a single transmission step 630, in contrast to setting up one connection to the centralized server for each acquired and encrypted mobile communication device identifier.

[0076] Fig. 7 is a flowchart showing steps of a method according to a further embodiment of the present invention. The method of Fig. 7 is for handling information regarding mobile communication devices used together with vehicles, and/or regarding vehicles used together with mobile communication devices, in a secured manner. In particular, the method is for handling the data acquired, encrypted and transmitted from a CID device according to the method of Fig. 6, e.g. on a centralized server.

[0077] As shown in Fig. 7, in step 710 one or more vehicle identification data sets are stored for each of one or more vehicles. Each vehicle identification data set comprises a vehicle identifier. The vehicle identification data sets are for instance the vehicle identification data sets acquired by an ANPR camera as used in the method of Fig. 1.

[0078] In step 720, one or more mobile communication device identification data sets are stored for each of one or more mobile communication devices. Each mobile communication device identification data set comprises a first and a second encrypted mobile communication device identifier generated with a first and a second encryption method, wherein the first encryption method uses a public key for encryption and requires a paired private key for decryption, and wherein the second encryption method uses a one-way mapping function such that the second encrypted mobile communication device identifier cannot be decrypted. The mobile communication device identification data sets are for instance the mobile communication device identification data sets acquired by a CID device as used in the methods of Fig. 1 or Fig. 6.

[0079] An example for the first encryption method is the above discussed RSA method. An example of the second encryption method is SHA (for Secure Hash Algorithm), which is based on cryptographic hash functions. A cryptographic hash function is a mathematical algorithm that maps data of arbitrary size to a bit string of a fixed size. It is designed to be a one-way function, that is, a function which cannot be inverted. Preferably, SHA is used with a 256-bit encryption key.

[0080] Similar to the methods of Figs. 2 and 3, the method of Fig. 7 allows identifying mobile communication devices used together with a vehicle. In particular, in step 730, a user input is acquired which specifies a vehicle identifier. In other words, the user can enter e.g. a plate number p. In step 740, at least one mobile communication device used together with a vehicle identified by the specified vehicle identifier is identified. This is done by means of the mobile communication device identification data sets and the vehicle identification data sets. Preferably, the identification is done using any of the methods as shown in Figs. 1 to 3 and discussed above, which allow a user to search for mobile communication devices that are associated with a vehicle specified by the user, and which further allow to determine a confidence score for each determined association.

[0081] In step 750, information regarding the identified at least one mobile communication device is outputted, e.g. provided to the user. The information can e.g. be the first and/or second encrypted mobile communication device identifier comprised in the mobile communication device identification data set of the identified at least one mobile communication device.

[0082] Further, similar to the methods of Figs. 4 and 5, the method of Fig. 7 allows identifying vehicles used together with a mobile communication device. In particular, in step 760 a user input is acquired which specifies a mobile communication device identifier, e.g. a CID as discussed above. If the mobile communication device identifier as provided by the user is not encrypted with the second encryption method, it is then encrypted in step 770, using the second encryption method, e.g. the above discussed SHA encryption method. Otherwise, i.e. if the mobile communication device identifier as provided by the user is already encrypted, the method continues with step 780. It should be noted that step 770 is necessary, because the mobile communication device identification data sets only comprise mobile communication device identifiers in RSA and SHA encrypted form, but not in unencrypted form. Further, an RSA-encrypted CID is not suitable for querying, while a hashed CID allows for an efficient, yet secure way of querying, as discussed above.

[0083] In step 780, at least one vehicle used together with the mobile communication device identified by the specified mobile communication device identifier is identified. This is done by means of the second encrypted mobile communication device identifiers comprised in the mobile communication device identification data sets and the vehicle identification data sets.

[0084] Finally, the vehicle identifier of the identified at least one vehicle is outputted in step 790, e.g. provided to the user.

[0085] Accordingly, the method as shown in Fig. 7 and as discussed above also allows identifying mobile communication

devices used together with a vehicle, or vice versa, however in a secured manner. In particular, storing both, SHA and RSA encrypted data, allows providing two levels of authorization: Non-authorized users can access the CID data through the hash version, meaning that they can get information on the associations between CID and plates, but will not see the real IMSI and IMEI. Thus, non-authorized users can search for a known mobile communication identifier, e.g. an IMSI, if they know it, by using the hashed data. It is noted that this kind of search works in a similar same way as password matching, and thus is very efficient. On the other hand, authorized users, like security authorities, will have access to the unencrypted data, e.g. through a security dongle providing the private key necessary to decrypt the data.

[0086] It should again be noted that hashed data cannot be decrypted, and thus for the purpose of providing encrypted data that can be decrypted by authorized users, RSA-encrypted data and hashed data are stored in parallel.

[0087] It should further be noted that preferably a mobile communication device identification data set does not comprise an unencrypted mobile communication device identifier of the respective mobile communication device, to ensure that the CID data is acquired and handled in a secured manner, to prevent unauthorized use thereof, even by the provider of the system or the server on which the data is stored.

[0088] In a practical example of the provided methods for identifying mobile communication devices used together with a vehicle, or vice versa, in a secured manner, assume that user "policeman A" wants to find information about an individual. Policeman A knows the corresponding IMSI, i.e. the mobile communication device identifier, of a mobile communication device used by that individual. Thus, Policeman A can use the unencrypted form of the IMSI as input for the in the search form, i.e. as user input specifying a vehicle identifier. The unencrypted IMSI as input by Policeman A will be hashed and compared to the hashed entries in the database as stored in the centralized server 810, to fulfill the search. As policeman A is not authorized to access decrypted data, he cannot access e.g. the IMSIs of all individuals that where at a location at a certain time.

[0089] In contrast, another user "detective B" is authorized to access decrypted data. Accordingly, if detective B wants to know the IMSIs in an area, he can provide the required private key for decrypting the data to the system, e.g. using a dongle with the private key. Alternatively, detective B may enter a password to get access to decrypted data. In case detective B performs a search by starting a query, all mobile communication device identifiers involved in that query are decrypted using the RSA private key.

[0090] In summary, the method of Fig. 6 is executed by a CID device, e.g. CID device 810 in Fig. 8. The CID device 810 starts by encrypting captured CID numbers with an asymmetric encryption algorithm, namely RSA with a key of 1024 bits, before transmitting the CID numbers to a centralized server, e.g. centralized server 820 in Fig. 9. At the centralized server 820, which preferably executes the method of Fig. 7, the transmitted RSA-encrypted CID numbers are decrypted with the respective private key (e.g. provided to the centralized server 820 by means of a dongle) corresponding to the device, and are immediately encrypted again, using RSA and SHA encryption.

[0091] The RSA encrypted CID numbers are used in case of a query wherein a user asks for decryption, providing that he is authorized. The hash (SHA) encrypted CID numbers are used for any query of a user (without special authorization) wherein the real HW ID is provided as query.

[0092] It is noted that the hash encrypted version of a CID number cannot be decrypted as SHA is a one-way function, as discussed above. A has value can however be used for querying the stored data. In contrast, the RSA encrypted version of a CID number cannot be used for querying the stored data, because the RSA encryption method, applied to a specific CID number as input, returns a different value each time it is applied. The reason is to prevent a brute force attack to RSA encrypted data. Accordingly, it is advantageous to store two encrypted versions of the CID numbers in the database stored in the centralized server 810, and thus the CID numbers are securely stored in the two different formats: the first being the RSA-encrypted format, the other is a hashed version of the data.

[0093] The table below shows what data is transmitted from the CID device(s), and what data is stored at the centralized server.

Captured	Sent	Stored in centralized server	Stored in centralized server
IMEI	$RSA_{1024}(IMEI)$	$RSA_{1024}(IMEI)$	$SHA_{256}(IMEI)$
IMSI	$RSA_{1024}(IMSI)$	$RSA_{1024}(IMSI)$	$SHA_{256}(IMSI)$

[0094] The advantage of the embodiments in which the CID device 810 provides only the RSA encrypted CID numbers is that the CID device 810 only needs to perform one encryption method, namely RSA, while the second encryption of the CID numbers, namely the hashed version using SHA, is performed by the centralized server 810. Accordingly, the CID device 810 needs less hardware resources and computing effort. This also allows to reduce the complexity and size of the CID device 810, leading to further effects, e.g. reduced power consumption and space requirements.

[0095] Alternatively, the captured CID numbers could be transmitted by the CID device in unencrypted form and then be encrypted on the centralized server, using both encryption methods. However, if the centralized server only receives

encrypted CID numbers, it can be ensured that not even the operator or provider of the server can access the CID numbers.

[0096] In a further alternative, according to further embodiments, the CID device 810 encrypts and transmits the acquired mobile communication device identifier using both, the first and second encryption methods, e.g. the RSA and SHA. Accordingly, in these embodiments the centralized server 810 is relieved of the burden to decrypt and encrypt the CID numbers. This is advantageous if the complexity of the centralized server 810 is limited, and further allows to use the resources of the centralized server 810 for other tasks.

[0097] As shown in Fig. 8, system 800 comprises a CID device 810 comprising means to carry out the steps as shown in Fig. 6. That is, CID device 810 is configured to capture CID numbers of nearby mobile communication devices. As discussed above, the captured CID data is preferably encrypted by the CID device 810, before being transmitted to a centralized server 820.

[0098] The centralized server 820 comprises means for carrying out the steps as shown in Fig. 7. That is, the centralized server 820 is configured to store the CID data as provided by CID device 810, wherein the CID data is stored in two encrypted forms, RSA and SHA, as shown in the table above.

[0099] Furthermore, system 800 comprises an ANPR camera 830 comprising means to carry out the steps of Fig. 1 relating to the acquiring of plate numbers.

[0100] In order to ensure that CID device 810 and ANPR camera 830 can capture data that can meaningfully be combined by the methods as discussed above, both devices are deployed next to a road. The ANPR camera 830 can preferably be mounted above the lanes of a road, to be able to capture images of passing vehicles.

[0101] Fig. 9 shows an alternative view of system 800. A scenario as shown in Fig. 9 is also referred to as an acquisition site. An acquisition site preferably comprises one CID device 810 and one or more ANPR cameras 830, preferably one ANPR camera per road lane. A CID device 810 preferably comprises a directional antenna which allows targeting the capture of the mobile communication devices to the road in line of sight. Both, the ANPR cameras 830 and the CID device 810 are connected to a network, e.g. the Internet, via a respective network interface. The data obtained by the ANPR cameras 830 and the CID device 810 are securely transmitted over the Internet to centralized server 820 and stored therein as discussed above. In case of several acquisition sites, the centralized server 820 gathers data from all these acquisition sites. The methods as discussed above and as shown in Figs. 1 to 5 and 7 are executed by the centralized server 820, i.e. obtaining and storing the vehicle and mobile communication device identification data sets and combining these data to identify mobile communication devices used together with a vehicle, and vice versa vehicles used together with mobile communication devices. In preferred embodiments, the entities of system 800 perform the above discussed methods in a secured manner.

[0102] It should be noted that the present invention is more efficient if used with more than one acquisition site. However, the present invention is not limited to a specific number of acquisition sites. In particular, the present invention is also efficient if used with one acquisition site used for an extended period of time, e.g. on several days.

[0103] Fig. 10 shows another alternative view of system 800. As shown in Fig. 10, CID device 810 comprises a device manager and a database DB for storing data acquired by the acquisition sites. According to the communication protocol used for communication with the interceptor, i.e. the centralized server 820, the CID device connects to the interceptor and creates a secure channel for transmitting data. At predetermined intervals, e.g. every five seconds, the CID device retrieves all new entries from the database, i.e. all new entries acquired in the meantime by the acquisition sites, encrypts the HW/SIM IDs, i.e. the mobile communication device identifiers using RSA and a public key of e.g. 1024 bits, and puts the entries in a list which is then sent together with their metadata, e.g. time and acquisition site, over the secured channel to the interceptor 820.

[0104] The interceptor 820 receives the data transmitted by the CID device 810 in a list. For each entry, the HW ID and SIM ID, i.e. the mobile communication device identifiers, are decrypted using the private key. Then the interceptor 810 generates RSA and SHA values for HW ID and SIM ID, which are then both stored in the local database maintained at the interceptor 820.

[0105] Although the invention has been explained in relation to its preferred embodiment(s) as mentioned above, it is to be understood that many other possible modifications and variations can be made without departing from the scope of the present invention. It is, therefore, contemplated that the appended claim or claims will cover such modifications and variations that fall within the true scope of the invention.

Claims

1. A method for identifying mobile communication devices used together with vehicles, or vehicles used together with mobile communication devices, the method comprising the steps of:

obtaining (110), for each of one or more vehicles, one or more vehicle identification data sets, each comprising a vehicle identifier and a vehicle identifier acquisition site, the vehicle identifier acquisition site comprising a

time and a location at which the vehicle identifier has been acquired;
 obtaining (120), for each of one or more mobile communication devices, one or more mobile communication device identification data sets, each comprising a mobile communication device identifier and a mobile communication device identifier acquisition site, the mobile communication device identifier acquisition site comprising a time and a location at which the mobile communication device identifier has been acquired;
 generating (130) a vehicle and mobile communication device association set, wherein each entry of the association set associates a vehicle identification data set and a mobile communication device identification data set and the vehicle identifier acquisition site comprised in the vehicle identification data set corresponds to the mobile communication device identifier acquisition site comprised in the associated mobile communication device identification data set; and
 based on the generated association set, identifying (140) at least one mobile communication device used together with a specified vehicle, or at least one vehicle used together with a specified mobile communication device.

2. The method of claim 1, wherein a vehicle identifier acquisition site corresponds to a mobile communication device identifier acquisition site if:

the location comprised in the vehicle identifier acquisition site corresponds to the location comprised in the mobile communication device identifier acquisition site; and
 the time comprised in the vehicle identifier acquisition site corresponds to the time comprised in the mobile communication device identifier acquisition site.

3. The method of claim 2, wherein the time comprised in a vehicle identifier acquisition site corresponds to the time comprised in a mobile communication device identifier acquisition site if the time comprised in the vehicle identifier acquisition site and the time comprised in the mobile communication device identifier acquisition site are within the same predefined time interval.

4. The method of any one of the preceding claims, further comprising:

acquiring (210) a user input specifying a vehicle identifier;
 determining (220) a vehicle identifier associated set of preferably all mobile communication device identifiers comprised in the mobile communication device identification data sets associated in the associated set with vehicle identification data sets comprising the specified vehicle identifier; and
 for each of the mobile communication device identifiers comprised in the vehicle identifier associated set, calculating (230) a confidence score for an association of the specified vehicle identifier with the mobile communication device identifier indicating a likelihood that the vehicle identified by the specified vehicle identifier has correctly been associated with a mobile communication device identified by the mobile communication device identifier.

5. The method of claim 4, wherein calculating (230) the confidence score for the association of the specified vehicle identifier with a mobile communication device identifier comprises:

determining (230-1), in the association set, a first number $A(p, cid)$, specifying a number of entries associating a vehicle identification data set comprising the specified vehicle identifier with a mobile communication device identification data set comprising the mobile communication device identifier;
 determining (230-2) a first ratio of the first number $A(p, cid)$ and a second number $|Tp|$, specifying a number of vehicle identification data sets comprising the specified vehicle identifier;
 determining (230-3) a second ratio of the first number $A(p, cid)$ and a third number $|Dcid|$, specifying a number of mobile communication device identification data sets comprising the mobile communication device identifier;
 and
 determining (230-4) the sum of the first ratio and the second ratio.

6. The method of any one of claims 1 to 3, further comprising:

acquiring (410) a user input specifying a mobile communication device identifier;
 determining (420) a mobile communication device identifier associated set of preferably all vehicle identifiers comprised in the vehicle identification data sets associated in the associated set with mobile communication device identification data sets comprising the specified mobile communication device identifier; and

for each of the vehicle identifiers comprised in the mobile communication device identifier associated set, calculating (430) a confidence score for an association of the specified mobile communication device identifier with the vehicle identifier indicating a likelihood that the mobile communication device identified by the specified mobile communication device identifier has correctly been associated with a vehicle identified by the vehicle identifier.

7. The method of claim 6, wherein calculating (430) the confidence score for the association of the specified mobile communication device identifier with a vehicle identifier comprises:

determining (430-1), in the association set, a first number $A(p, cid)$, specifying a number of entries associating a vehicle identification data set comprising the vehicle identifier with a mobile communication device identification data set comprising the specified mobile communication device identifier;
determining (430-2) a first ratio of the first number $A(p, cid)$ and a second number $|Tp|$, specifying a number of vehicle identification data sets comprising the vehicle identifier;
determining (430-3) a second ratio of the first number $A(p, cid)$ and a third number $|Dcid|$, specifying a number of mobile communication device identification data sets comprising the specified mobile communication device identifier; and
determining (430-4) the sum of the first ratio and the second ratio.

8. The method of claims 5 or 7, respectively, wherein calculating the confidence score comprises multiplying the sum with a factor, preferably 0.5.

9. The method according to any one of the preceding claims, further comprising the steps of acquiring, for each of the one or more vehicles, the one or more vehicle identification data sets, and/or acquiring, for each of one or more mobile communication devices, the one or more mobile communication device identification data sets.

10. The method of claim 9, wherein acquiring a vehicle identification data set for a vehicle comprises:

capturing an image of the vehicle with a camera (830); and
processing the captured image with image processing to extract license plate data associated with a license plate of the vehicle.

11. The method of claim 10, wherein the camera (830) is configured for Automatic Number Plate recognition, ANPR, or for Automatic License Plate recognition, ALPR.

12. The method of claim 9, wherein acquiring a mobile communication device identification data set for a mobile communication device comprises capturing at least one identification of the mobile communication device by a capturing device (810), preferably one of a base station operating according to a standard for wireless communication.

13. The method of claim 12, wherein an identification of the mobile communication device captured by the capturing device (810) is:

an identifier associated with a subscriber module comprised by the mobile communication device; or
an identifier associated with the mobile communication device.

14. The method of any of claims 13 or 14, wherein acquiring a mobile communication device identification data set for a mobile communication device further comprises:

querying a mobile communication device identification server with at least one of the captured identifications; and
in response, receiving, from the mobile communication device identification server, the mobile communication device identifier identifying the mobile communication device.

15. A system (800) for identifying mobile communication devices used together with vehicles, or vehicles used together with mobile communication devices, the system comprising means configured for carrying out the steps of the method of any one of claims 1 to 14.

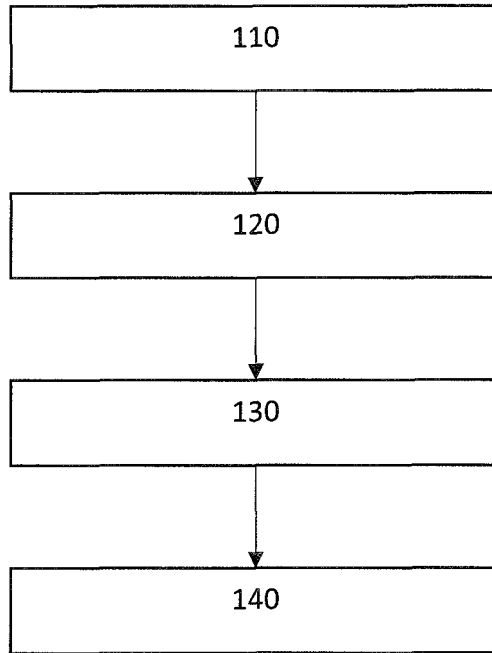


Fig. 1

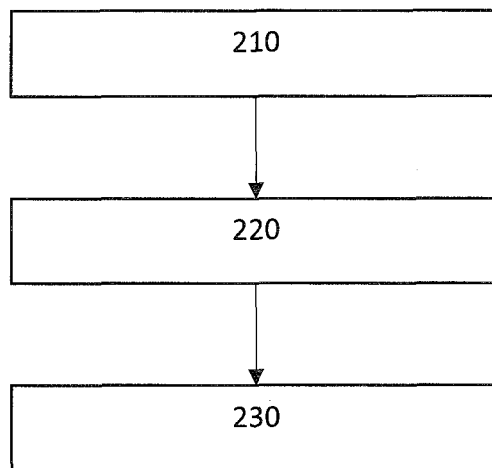


Fig. 2

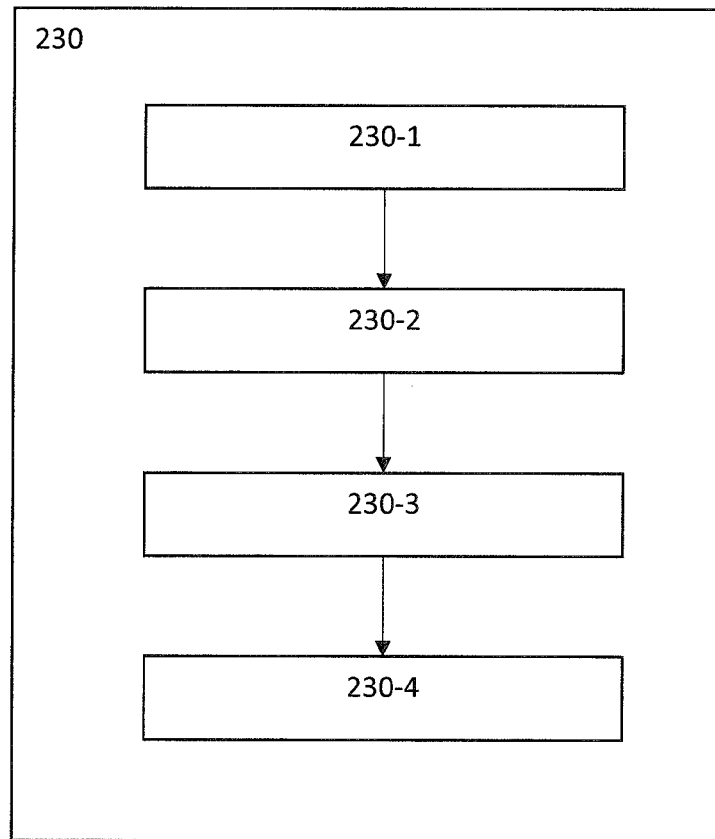


Fig. 3

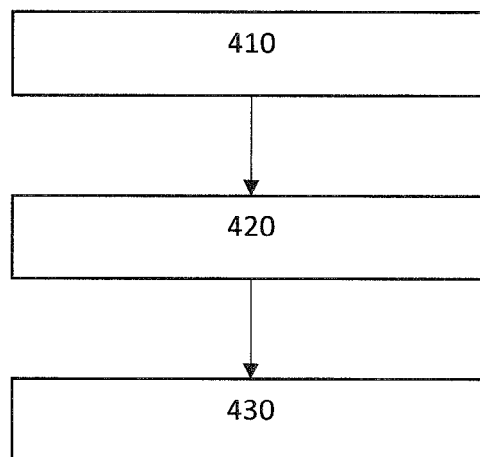


Fig. 4

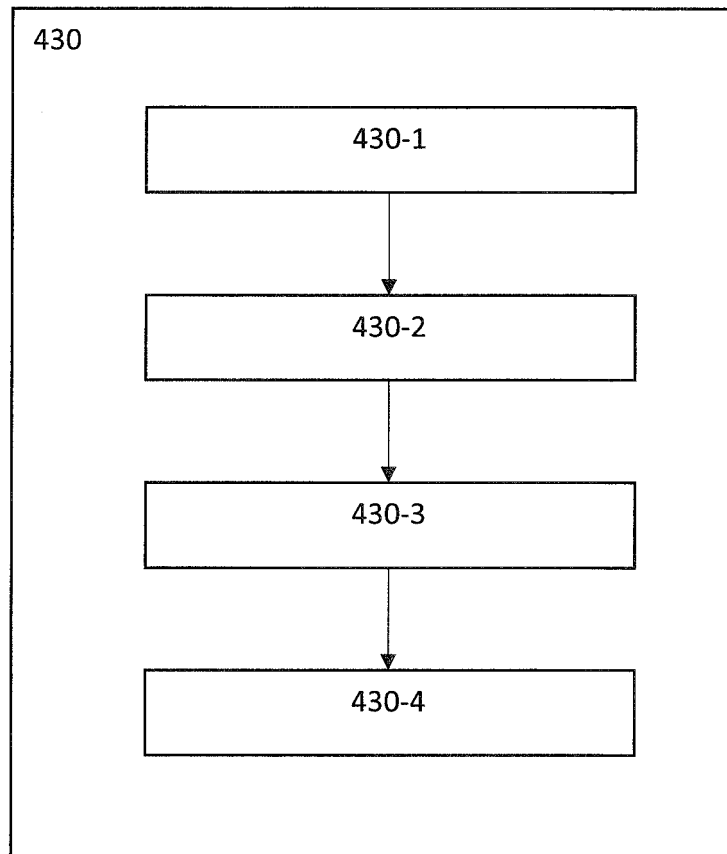


Fig. 5

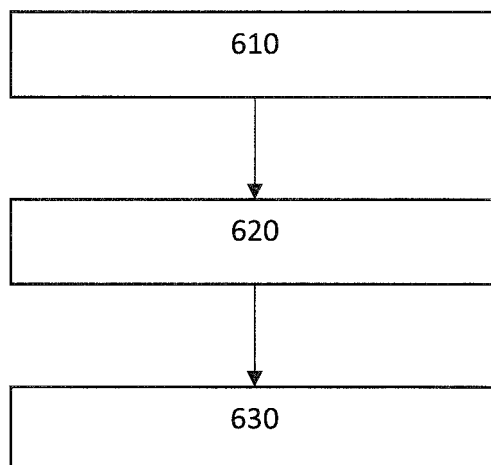


Fig. 6

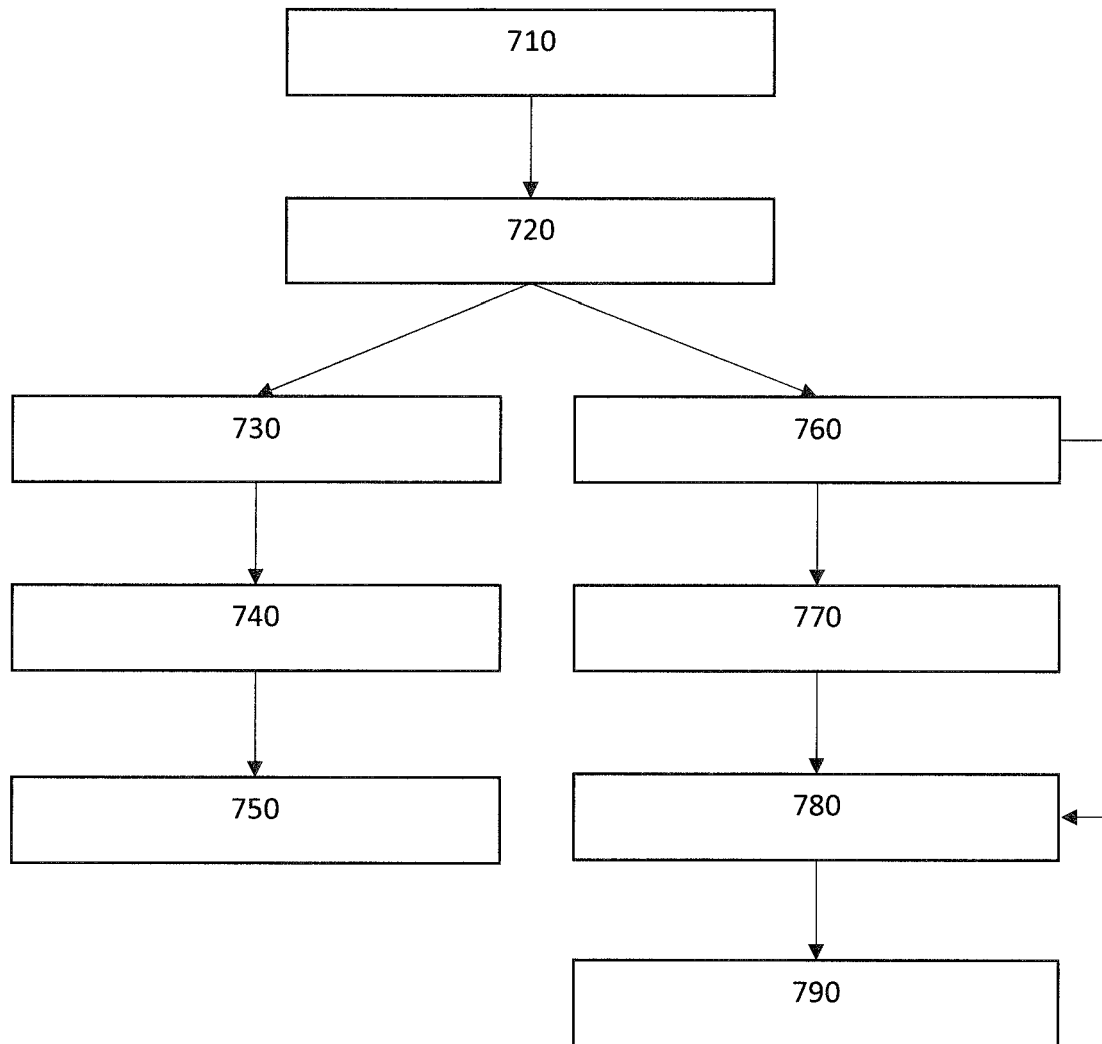


Fig. 7

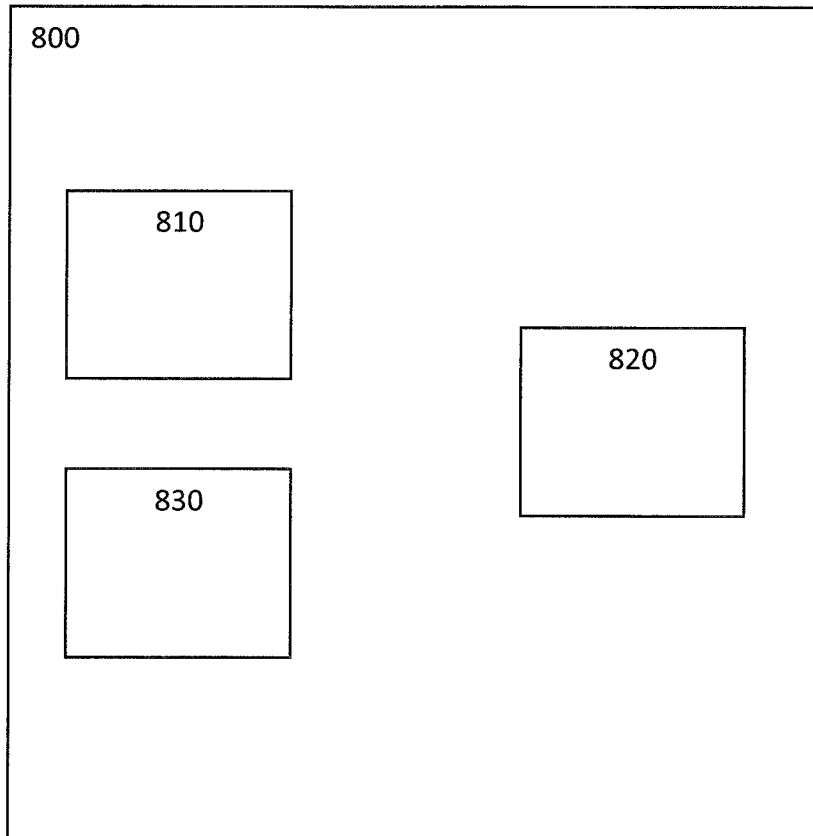


Fig. 8

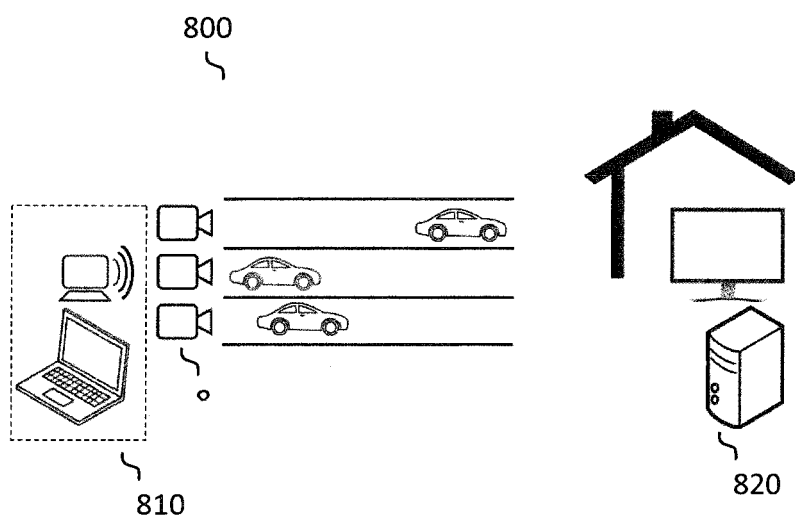


Fig. 9

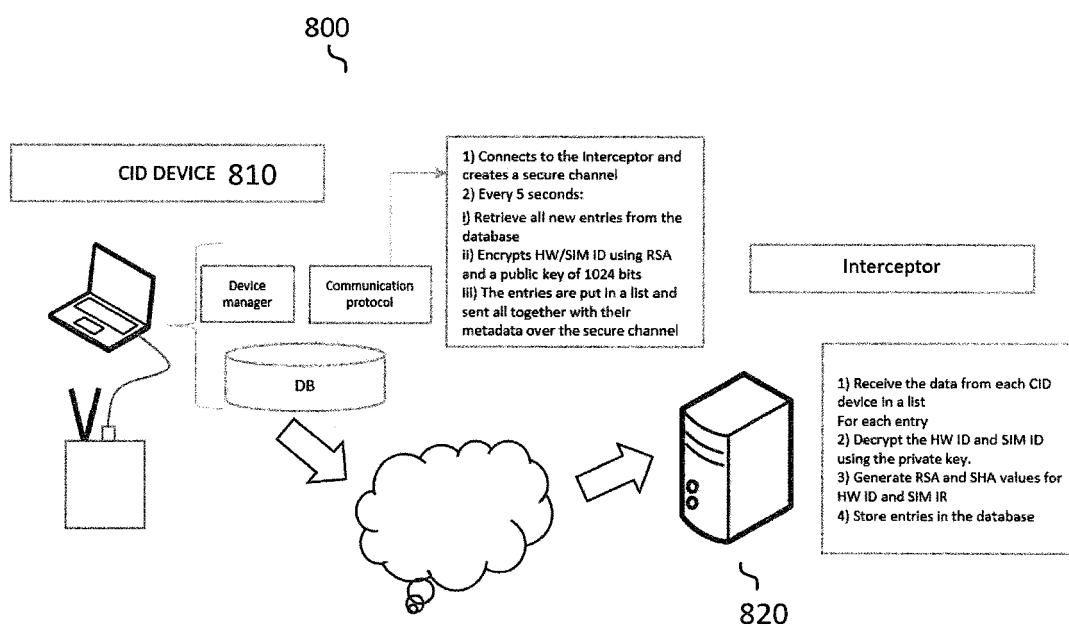


Fig. 10



EUROPEAN SEARCH REPORT

Application Number
EP 16 19 2155

5

10

15

20

25

30

35

40

45

50

55

1

EPO FORM 1503 03.82 (P04C01)

DOCUMENTS CONSIDERED TO BE RELEVANT			
Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (IPC)
X	WO 2014/072971 A1 (GIVON ASSAF [IL]; ATAD YOTAM [IL]) 15 May 2014 (2014-05-15)	1-3,9-15	INV. G08G1/01 G08G1/017
A	* abstract; figures * * page 3, line 22 - page 4, line 22 * * page 5, line 28 - page 6, line 1 * * page 7, line 30 - page 8, line 20 * * page 9, line 10 - page 10, line 13 *	4-8	
A	WO 2016/055226 A1 (KAPSCH TRAFFICOM AG [AT]) 14 April 2016 (2016-04-14) * abstract; figures * * page 7, line 10 - line 24 * * page 8, line 7 - line 16 * * page 9, line 8 - line 22 * * page 10, line 25 - page 11, line 27 * * page 14, line 1 - line 11 *	1-15	
A	WO 2012/013228 A1 (TRAFFIC NETWORK SOLUTIONS S L [ES]; NORDENTOFT ROBERT [ES]; GARRIDO GO) 2 February 2012 (2012-02-02) * abstract; figures * * page 5, line 7 - line 19 *	1-15	TECHNICAL FIELDS SEARCHED (IPC) G08G
The present search report has been drawn up for all claims			
Place of search The Hague		Date of completion of the search 7 April 2017	Examiner Roost, Joseph
CATEGORY OF CITED DOCUMENTS X : particularly relevant if taken alone Y : particularly relevant if combined with another document of the same category A : technological background O : non-written disclosure P : intermediate document T : theory or principle underlying the invention E : earlier patent document, but published on, or after the filing date D : document cited in the application L : document cited for other reasons & : member of the same patent family, corresponding document			

**ANNEX TO THE EUROPEAN SEARCH REPORT
ON EUROPEAN PATENT APPLICATION NO.**

EP 16 19 2155

5

This annex lists the patent family members relating to the patent documents cited in the above-mentioned European search report.
The members are as contained in the European Patent Office EDP file on
The European Patent Office is in no way liable for these particulars which are merely given for the purpose of information.

07-04-2017

10

15

20

25

30

35

40

45

50

55

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 2014072971 A1	15-05-2014	NONE	
WO 2016055226 A1	14-04-2016	CA 2867173 A1 WO 2016055226 A1	07-04-2016 14-04-2016
WO 2012013228 A1	02-02-2012	ES 2424397 A2 WO 2012013228 A1	01-10-2013 02-02-2012

EPO FORM P0459

For more details about this annex : see Official Journal of the European Patent Office, No. 12/82