

SYSTEM AND METHOD FOR MONITORING VEHICLES AND DRIVERS

FIELD OF THE INVENTION

The present invention is in the field of vehicle and driver monitoring; more specifically the present invention is related to a method and system for remotely verifying the identity of a driver and the validity of his/her driving license, insurance status and vehicle documents without the need to stop the vehicle for inspection.

BACKGROUND OF THE INVENTION

Car accidents and thefts are common events in most countries. It is up to law enforcement and other authorities to keep some form of control in the transportation arena. In order to exercise control over the automotive world, drivers are typically obliged by law to hold three driving regulatory documents (DRD): a valid driver's license issued by the state to the actual driver, a valid car registration and a valid insurance policy.

Typically it is the police that is engaged in enforcing the law and monitoring drivers. However, the ability of police to enforce the laws is limited. The police force usually opts to check one or more vehicles or the validity of driver documentation, for example, by random sampling at specific locations by pulling them over and visually inspecting the aforementioned documents. However, many drivers use forged documents in order to avoid paying the licensing and insurance fees. One way to verify a suspicious car or driver

would be to run the actual serial numbers of the driver's license and the vehicle registration through a main computer system to verify whether they are indeed authentic. Even then, to verify the legitimacy of an insurance policy the actual insurance agency would need to be contacted.

The above situations leave both the police and the state with the following afflictions. A large number of vehicles without valid registration and approval to being operated on the roads. A large number of drivers do not hold a valid drivers license and some even drive under suspension. A large number of drivers are driving without valid insurance. These issues originated from the inability to monitor and validate regulatory documents of the vehicles while travelling, consequently costing thousands of lives and billions of dollars.

Systems for electronic identification of vehicles from a distance are known in the art. International patent application WO98/30421 discloses a vehicular disablement method and apparatus, in which police can identify and stop a vehicle that is attempting to flee from a traffic stop. The apparatus includes an interrogator system located in a law enforcement vehicle and a responder system located in a target vehicle.

US 7,352,290 (Eskridge) describes a system installed in patrol vehicles such as highway patrol, or local police patrol. The system uses wireless technologies to scan and compare VIN (vehicle identification numbers) with license plate against the Department of Motor Vehicles database, and against the local police database for outstanding warrants. All passing cars would be processed. The system then displays the information on the patrol car's computer system, and notifies the police officer of any outstanding warrants, if the car is stolen, and if there is a problem with the registration or tags on the vehicle. The system may also include a means to record the finger print of a driver after the driver has been stopped by a police patrol person.

In US 7,352,290 (Eskridge), a traffic speed surveillance system is provided by a set of monitor transceivers located along a roadway and communicating with a central processor, and including at least some stationary transceivers sending radio signals indicative of speed limit in the location of the particular stationary transceiver. A vehicle transceiver mounted in a vehicle includes means for entering driver identification and vehicle identification, and speedometer means for measuring the speed of the vehicle. The vehicle transceiver receives the radio signals from the monitor transceiver indicative of speed limit and compares measured speed against the limit, and sends radio signals indicative of driver identification, vehicle identification and speed limit violation to the monitor transceiver for reporting to the central processor.

SUMMARY OF THE INVENTION

Accordingly, it is an object of the present invention to provide a system and method including at least one of the following: an efficient and useful means for monitoring drivers and vehicles; use of a biometric feature to allow remote confirmation that the driver is indeed the person to whom the driving license was granted; use of a biometric feature to allow remote confirmation that the driver is legally allowed to operate a vehicle of the type being operated (e.g. a truck, bus, taxi, manual transmission, etc., or a person with a "youth" license driving after permitted hours for such a license, and so on) and use of a biometric feature to remote access the driving history (e.g. drunk driving, speeding issues, and the like), or any other documented issues, of the driver.

According to one aspect of the present invention, there is provided a system for inspecting driving regulatory documents, the system comprising: at least one storage medium associated with a vehicle for storing driver and vehicle data; an electronic documentation retrieval and transmitter for reading data from the storage medium and transmitting information signals; and a law enforcement interrogator device adapted to interrogate and receive the information signals, wherein the driver data comprises at least one biometric feature for confirming the identity of the driver.

According to another aspect of the present invention, there is provided a method for inspecting driving regulatory documents, the method comprising: storing driver and vehicle data in at least one storage medium; reading data from the storage medium by an electronic documentation retrieval and transmitter; and transmitting from the electronic documentation retrieval and transmitter to a law enforcement interrogator device compliant or noncompliant information, wherein the driver data comprises at least one biometric feature for confirming the identity of the driver.

DETAILED DESCRIPTION OF EMBODIMENTS OF THE INVENTION

Implementing the system and method of the present invention enhances the ability to discern non compliance of DRDs in a vehicle. The law-enforcement agent using the system and method is able to remotely identify vehicles having faulty DRDs. According to some embodiments, the hard copies of the DRDs are supplemented or altogether replaced by a digital storage medium containing relevant stored data. The storage medium can be installed in the driver's car or the data may be stored in a centralized law enforcement database. The police may access the database in order to retrieve information regarding the validity of the driver's permits. In the scenario wherein the digital storage medium is located in the driver's car, typically one or more smart cards, RFID cards or flash memory devices or discs may be used to store the current data. Such memory devices are referred to hereinafter as digital memory cards (DMCs). The DMCs each carry a verification code to indicate that the permits have been issued and are valid. The cards that are placed in the driver's car connect to a transceiver unit that transmits the data relating to the validity of the car registration, driver license

and insurance policy, typically to a range of several meters. The law enforcement agent is equipped with a compatible transceiver or law enforcement interrogating device (LEID). The device is able to determine if the data received from a specific driver's vehicle electronic documentation retrieval and transmitter (EDRT) matches the data expected, as obtained in a local database in the EDRT, or by searching in a related database such as a police database, the access to which is made by the LEID. Data referring to stolen vehicles and suspended driving licenses are examples of data stored in the LEID. Vehicles/drivers bearing incompliant data would then be subjected to further interrogation by the law enforcement agent. The driver's car transceiver typically first reads the information stored on the cards and then transmits a communication containing information relating to those cards. A signal indicating compliant information sent by the vehicle and received by the LEID triggers, for example, a display on a monitor of the LEID that "vehicle and driver information are valid". Incompliant information sent by the vehicle or lack of information received by the LEID triggers, for example, a display on a monitor of the LEID that "vehicle and driver information invalid". Optionally the transmission of a signal related to compliant and/or incompliant information will disclose the driver's name or any other pertinent details and alert the LEID whether the vehicle has been stolen.

According to preferred embodiments, the vehicle's transceiver and the driver's license card have a biometric fingerprint feature. Upon receiving the driving license card the driver's fingerprint is irreversibly imprinted on his/her card. Once the driver wishes to drive a vehicle he/she will insert the card into

the driver's car transceiver which will then request/require that the driver place his/her finger on the transmitter biometric recognition plate. If the driver's fingerprint matches the fingerprint stored in the card memory, the system will send compliant information.

Another optional feature is a specific definition as to the type of vehicle the driver is allowed to use (e.g. commercial, passenger, manual transmission, etc.) and under what conditions (such as young drivers required to be accompanied by an adult). In addition, the invention can be used to remotely identifying a driver with a criminal/drunk record or other suitable issues. In case the driver's license definitions do not match other system parameters such as vehicle type or insurance definition the system will not transmit the compliant information signal. In order for the system to work, the three cards will need to be connected to vehicle's information (data) unit at the beginning of each driving event and the driver's card is typically removed at the end of the drive. Each of the cards is issued to the driver and the vehicle upon payment, at the appropriate renewal time; optimally the DRDs may be kept separately by the vehicle's owner or driver. Once the cards are installed in the EDRT, the EDRT's processor will read the information stored on the cards. When a law enforcement agent equipped with LEID sends an interrogation signal to the vehicle, the vehicle will respond with a transmission of a compliant or noncompliant information signal or may not transmit any signal. Once the validity of the card expires (e.g. when the insurance expired or when it is time to issue a new driver's license or car registration) the card invalidates and the driver/car owner is obliged to renew the validity. Typically, and as required by the local authorities, the cards are to include all the information of the current paper permits, such as driver's age, vehicle type, etc. In case a driver is found violating the local requirements, the law enforcement agent may be empowered to either update the database regarding the new situation e.g. that the driver has an invalid licensing or issue the driver a temporary DMC.

An exemplary application of the invention is wherein a vehicle is stopped for an infraction such as a broken headlight. Here, the policeman can access the card (or the storage medium, depending upon where the data is located) and re-program it so that, for example, the expiry date is in a week, whereby the vehicle need be repaired within a week, at which point the card/storage medium would be re-programmed to the original expiry date.

Electronic documentation retrieval and transmitter

The driver's car electronic documentation retrieval and transmitter (EDRT) is typically installed behind the vehicle's windshield. The EDRT can be typically encrypted and installed only once. The memory unit/s of the EDRT include/s encrypted data such as, a unique code of the vehicle, vehicle licensing number, vehicle identification number (VIN), and the annual due date of a mandatory safety check (if applicable). The EDRT further includes a processor such as microcontroller for reading the information on the smart cards and a short-range transmitter. Preferably the EDRT transmits RF signals. The EDRT includes a receiver to receive interrogation signals from the LEID. The EDRT further includes connectors or slits for installing the three cards. The EDRT further includes an electrical power source such as a photoelectric cell, a connector to car battery and or a rechargeable battery back up. The EDRT further includes an audio or light indicator such as led to alert the driver in case of a missing card in one of the slits, a non-valid card or card that has expired.

The digital memory cards (DMCs)

In accordance to a preferred embodiment of the present invention, the system includes three cards: driver's license card, car registration card and insurance policy card.

The driver's license card represents the DRD driving license. The card is issued or updated at the same time that the DRD driving license is issued. Preferably the driver's license card further includes a biometric fingerprint of the driver. The card is valid when inserted in the appropriate slit of the EDRT and the fingerprint in the card matches the driver fingerprint read by the EDRT finger print reader. The card stores an encrypted data such as driver's license number, driver ID, date of driver license renewal, expiration date and type of the driving license.

The car registration card is issued with the DRD car registration license. The card stores an encrypted data such as licensing number, VIN, date of registration license renewal, expiration date and other conditioning data regarding to the type of the vehicle. The card can be valid and the EDRT can sent a compliant signal when the card is installed in the appropriate transmitter and when the encrypted data of the card is matched with data stored in the EDRT or in a central database such as central police, insurance and ministry of transportation database or federal database. For example, a unique code of the vehicle is kept in the car registration card and only when there is a matching between the data in the card and data in the EDRT, the EDRT will transmit a valid signal.

The insurance policy card is issued at the time the DRD insurance policy is issued. The card stores encrypted data such as registration number, VIN, date of insurance policy renewal and other conditioning data regarding to the type of the vehicle. The card can be valid and the EDRT can sent a compliant signal when the card is installed in the appropriate transmitter and when the encrypted data of the card is matched with data stored in the EDRT or in a central database such as central police, insurance and ministry of transportation database or federal database.

Law enforcement interrogating device (LEID)

The LEID includes a memory unit, a processor, a decrypter a transceiver and a power source. The LEID sends interrogation signal which is received by the EDRT of the inspected car, the device is provided with a memory for storing for example information about driving licenses that are not valid or suspended driving license. The device may be further provided with memory for storing information about stolen vehicles including stolen vehicles with installed cards in the EDRT. In one embodiment the information stored in the memory of the LEID can be downloaded and updated on-line from the relevant database authorities such as police database, database of ministry of transportation, database of the department of motor vehicle, database of the insurance policies and/or any federal authorities. The LEID may further include a biometric finger print means for matching a driver's fingerprint when stopped for inspection by a policeman with a datum of his fingerprint that is stored in the database of the law enforcement authority. Such a feature could be useful for example to detect drivers who are driving a vehicle from a

different class than permitted by their license, drivers with a license that has been revoked and even drivers of a stolen vehicle.

BENEFITS OF THE PRESENT INVENTION

The implementation of the system and method in accordance with the present invention will contribute both to law enforcement and public safety. The moving vehicles are continuously monitored within transmitting range of a policeman equipped with the system. The policeman is able to focus exclusively on unauthorized and therefore potentially unsafe vehicles or unlicensed drivers and pull them over with greater efficiency. The system will detect vehicles without valid insurance and aid in fighting vehicle theft. Using the system of the invention, the law enforcement officer's time will be much better utilized as a result of the ability to focus on violators only. The law-obeying drivers will be spared the inconvenience associated with disturbance and discomfort of random vehicle inspection.

The invention is particularly advantageous for travelling vehicles, however, much information can be derived from a parked vehicle, even if the driver is not present. Furthermore, the invention is particularly useful for use in police patrol vehicles, however it can be used in a static apparatus (e.g. attached to a roadside structure) or a handheld/portable device.

CLAIMS

1. A system for inspecting driving regulatory documents (DRDs), said system comprising:
 - a law enforcement interrogator device (LEID) to determine which vehicle needs to be pulled over by law enforcement agent for further inspection;
 - at least one storage medium for storing personal driver and driver's car data;
 - a driver's car electronic documentation retrieval and transmitter (EDRT) for reading data from said storage medium and transmitting to LEID compliant or noncompliant information signals to said LEID.
2. A system for inspecting driving regulatory documents (DRDs), as in claim 1, wherein said storage medium is a smart card.
3. A system for inspecting driving regulatory documents (DRDs), as in claim 1, wherein said at least one storage medium is updated with the current data of said regulatory documents.
4. A system for inspecting driving regulatory documents (DRDs) as in claim 1, wherein said storage medium is located in a law enforcement database.

5. A system for inspecting driving regulatory documents (DRDs) as in claim 1, wherein said storage medium is an RFID card.
6. A system for inspecting driving regulatory documents (DRDs) as in claim 1, wherein said system further comprises a central database for personal driver and driver's car data.
7. A system for inspecting driving regulatory documents (DRDs) as in claim 6, wherein said central database is a collection of data bases of central police, insurance and ministry of transportation databases, database of the department of motor vehicle or federal database and wherein said databases shared information on a driver and driver's car.
8. A system for inspecting driving regulatory documents (DRDs) as in claim 1, wherein said LEID is updated on-line with said database.
9. A system for inspecting driving regulatory documents (DRDs) as in claim 1 wherein the information on the driver's fingerprint is stored on at least one of said storage medium.
10. A system for inspecting driving regulatory documents (DRDs) as in claim 1 wherein said EDRT further uses biometric reader.
11. A system for inspecting driving regulatory documents (DRDs) as in claim 1 wherein said LEID further use biometric reader.

12. A method for inspecting driving regulatory documents (DRDs), said method comprises:

- Storing driver and driver's car data in at least one storage medium
- Reading data from storage medium by an electronic documentation retrieval and transmitter (EDRT)
- Transmitting from said EDRT to a law enforcement interrogator device (LEID) compliant or noncompliant information.

13. A method for inspecting driving regulatory documents (DRDs) as in claim 12, wherein said LEID is communicated with a central database.

14. A method for inspecting driving regulatory documents (DRDs) as in claim 12, wherein said storage medium is located in law enforcement data base.

15. A method for inspecting driving regulatory documents (DRDs) as in claim 12, wherein said data stored on said storage medium are encrypted.

16. A method for inspecting driving regulatory documents (DRDs) as in claim 12 wherein said method further comprising a biometric means for driver finger print matching.

17. A method for inspecting driving regulatory documents (DRDs) as in claim 12 wherein said LEID further uses a biometric reader.

18. A method for inspecting driving regulatory documents (DRDs), as in claim 12, wherein said at least one storage medium is updated with the current data of said regulatory documents.