

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Provisional Patent Application

A SYSTEM FOR ENHANCING NATIONAL SECURITY

Inventor:

Shailesh Kadakia

Reference No. 100-001-PRV

A SYSTEM FOR ENHANCING NATIONAL SECURITY

Technical Field

[0001] The invention relates generally to security systems including identification verification and sensing elements, and more particularly to employing ‘smart card’ technologies, biometric identification information, a central intelligence database, and explosives-sensing equipment.

Background

[0002] Terrorism is one of the most significant dangers facing the United States today. Since the terrible tragedy of September 11, 2001, vast resources have been expended in order to combat this danger. Nevertheless, it seems that progress has been slow in the field of verification of identity, as the use of paper, plastic, and other non-electronic passports and other government-issued identification cards (such as drivers’ licenses) continues.

[0003] These antiquated identification cards (IDs) have many problems. For example, many IDs are susceptible to simple forgery – from the eighteen-year-old who alters his brother’s ID so as to enter the corner pub, to the potential terrorist who purchases a fraudulent passport and travels between countries. Furthermore, the identification cards contain very little information about their subject, often limited to name, address, age, hair and eye color, weight, and height. Thus, it can

be difficult for law enforcement to verify that the person holding the ID card is in fact the individual named on that card.

[0004] An additional problem with current security methods is that they mainly utilize simple, non-networked metal-detecting devices. For example, when a traveler passes through a standard security checkpoint at an airport in the United States, he or she is screened by a simple metal detector and not an explosives detector. Occasionally, a piece of carry-on baggage may be selected for explosives screening, but the travelers themselves are not directly tested.

Summary

[0005] The technology described herein provides a method for enhancing the identification verification and screening processes at security checkpoints.

Detailed Description

[0006] In one implementation, the system offers the capability of utilizing advanced biometric identification methods through the use of smart card technologies. In another implementation, the system uses explosives sensing technologies to automatically screen passengers and their baggage. In yet another implementation, the combination of smart card technologies and explosives screening is enhanced via a computer network and central database. In this combined process, both traveler and baggage are automatically linked together and

information concerning both are shared with a central computer database at each security checkpoint through which they pass.

[0007] A significant benefit of this system is that both the traveler and his luggage are continuously linked by the network such that if there is a security concern with any piece of luggage or with the traveler himself, security personnel can easily locate and detain the traveler and all of his luggage.

[0008] One manifestation of the system is its implementation at ports of entry into the United States. All incoming travelers would be issued a smart card in place of, or in addition to, a passport. The card would contain enhanced identification information including travel history, employment history, identifying marks or characteristics, and biometrics such as fingerprints, retinal scans, voice-prints, video files, etc. As the technologies for scanning a person becomes practical, the various scanning devices can be implemented on an as-needed basis. For example, a small, inexpensive fingerprint scanning device is currently available and could be quickly and easily rolled-out to security checkpoints, whereas retinal scanning technology may not yet be cost-effective to implement. Nevertheless, because the smart card technology is able to store vast amounts of information, each traveler can be identified to a much greater degree than with current IDs. Whenever a traveler passes a security checkpoint, the smart card can be read and verified via comparison with the traveler and with a central database.

[0009] The security enhancements afforded by the smart card technologies are significant, especially when the security checkpoints are linked via a network to a central computer database. The data that is stored on the smart cards can be heavily encrypted and since it is verified with the central database, it can be kept secure.

[0010] When a traveler enters the security system by passing through a security checkpoint, his identification information is verified and he is linked in the system with any luggage he might be carrying. All pieces of luggage for a traveler can be linked to the traveler via a smart tag system using printed barcode labels, radio ID tags, or some other method. Then, when either the luggage or a traveler is screened at a security checkpoint, a security issue with any piece of luggage or with the traveler himself will cause a red flag to be assigned to the traveler and luggage so that both can be easily detained.

[0011] An additional security enhancement is the networked sensing devices that are added to the system, including explosives screening equipment. Such equipment would utilize advanced explosives sensing technologies including irradiation and spectral analysis.

[0012] In another implementation of the system, the smart card identification IDs could be issued in place of social security cards. The technologies necessary to mass produce inexpensive smart cards are already in place as evidenced by the smart cards in use as credit cards by the American Express Company, New York, New York.

[0013] The system of smart cards could also be expanded to all United States citizens as a replacement for other current forms of government-issued IDs such as drivers' licenses.

[0014] One high-level implementation of the system is shown in Figure 1 below. This particular implementation has the following ten primary components: (1) smart card, (2) issuance of smart card to person, (3) upload of information to central database, (4) contact between person and security checkpoint, (5) smart card read and verified against central database, (6) luggage identification tags attached to luggage, (7) traveler and luggage scanned by explosives detection devices, (8) information exchanged with central database, and traveler either (9) passes through security, or (10) traveler is detained.

[0015] The above specification, examples and data provide a complete description of the structure and use of exemplary implementations of the described articles of manufacture and methods. It is important to note that many implementations can be made without departing from the spirit and scope of the invention.

[0016] In some implementations, articles of manufacture are provided as computer program products. One implementation of a computer program product provides a computer program storage medium readable by a computer system and encoding a computer program. Another implementation of a computer program product may be provided in a computer data signal embodied in a carrier wave by a computing system and encoding the computer program.

[0017] Furthermore, certain operations in the methods described above must naturally precede others for the described method to function as described. However, the described methods are not limited to the order of operations described if such order sequence does not alter the functionality of the method. That is, it is recognized that some operations may be performed before or after other operations without departing from the scope and spirit of the invention.

Claims

WHAT IS CLAIMED IS:

1. A method for enhancing national security, the method comprising:
receiving one or more characteristics of a person, wherein each characteristic contains data describing the physical appearance of the person, the history of the person, or other identifying information about the person;
processing the characteristics into encrypted digital data;
encoding the digital data onto a smart card device;
communicating with a central computer database to verify and update any records concerning the person on the central database; and
issuing the smart card device to the person.
2. The method of claim 1 wherein the method further comprises:
contact between the person and a security checkpoint;

reading the smart card device in order to verify the identifying information on the smart card device; and

communicating with the central database in order to determine whether to detain the person or allow the person to continue through the security checkpoint.

3. The method of claim 2 wherein the method further comprises:
allowing the person to continue through the security checkpoint;
issuing one or more luggage identification devices to the person;
attaching the luggage identification devices to any luggage of the person;
contact between the person and a second security checkpoint;
scanning the person and the luggage for explosives; and
either detaining the person and the luggage or allowing the person to continue through the second security checkpoint.

4. The method of claim 2 wherein the method further comprises:
allowing the person to continue through the security checkpoint;
contact between the person and a second security checkpoint;
scanning the person for explosives; and
either detaining the person or allowing the person to continue through the second security checkpoint.

5. A method for enhancing national security, the method comprising:
receiving one or more characteristics of a person, wherein each characteristic contains data describing the physical appearance of the person, the history of the person, or other identifying information about the person;
processing the characteristics into encrypted digital data;
encoding the digital data onto a smart card device;
communicating with a central computer database to verify and update any records concerning the person on the central database; and
issuing the smart card device to the person as a replacement for an identification card.

6. The method of claim 5 wherein the identification card is a social security card.

7. The method of claim 5 wherein the identification card is a driver's license.

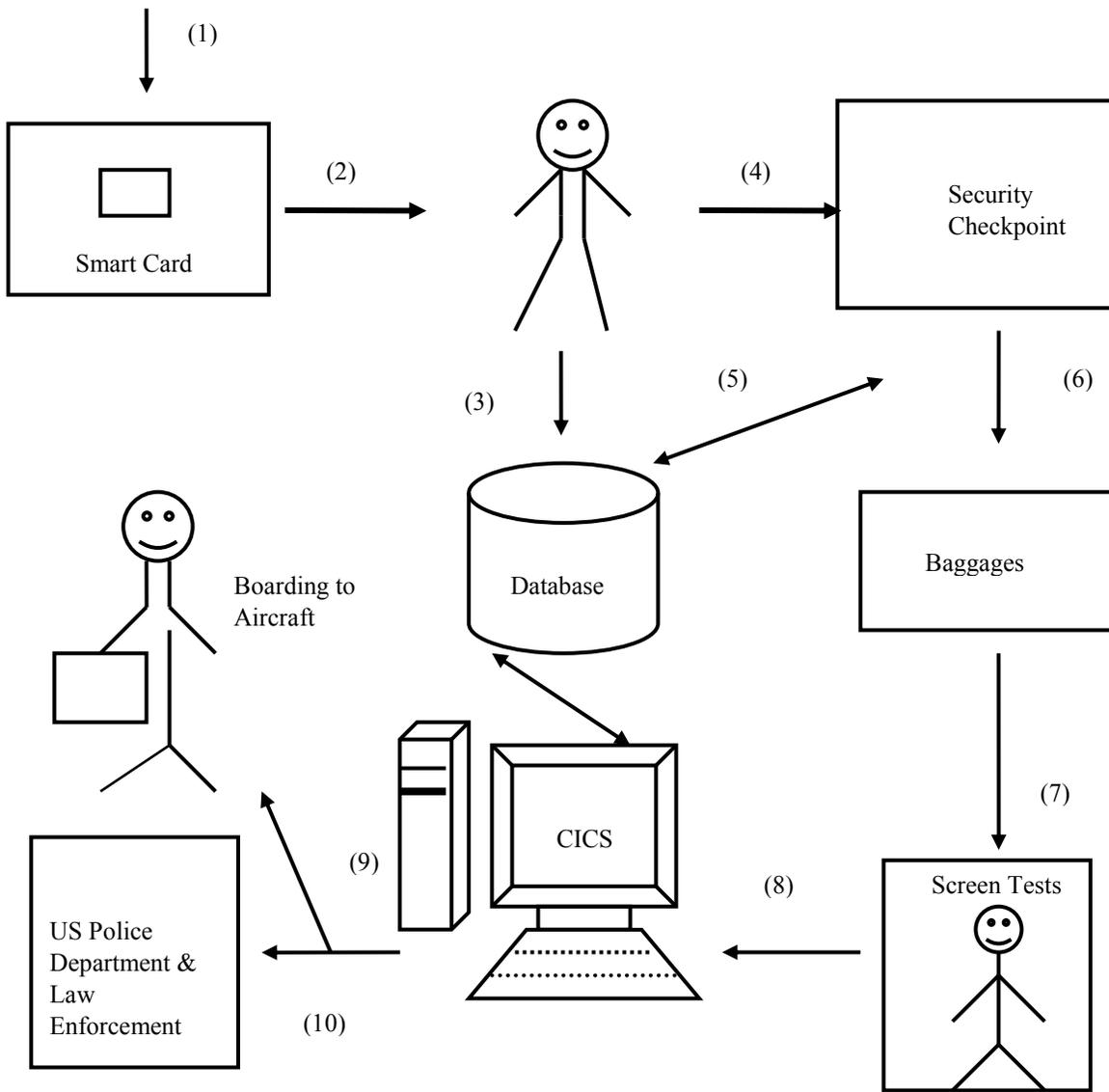
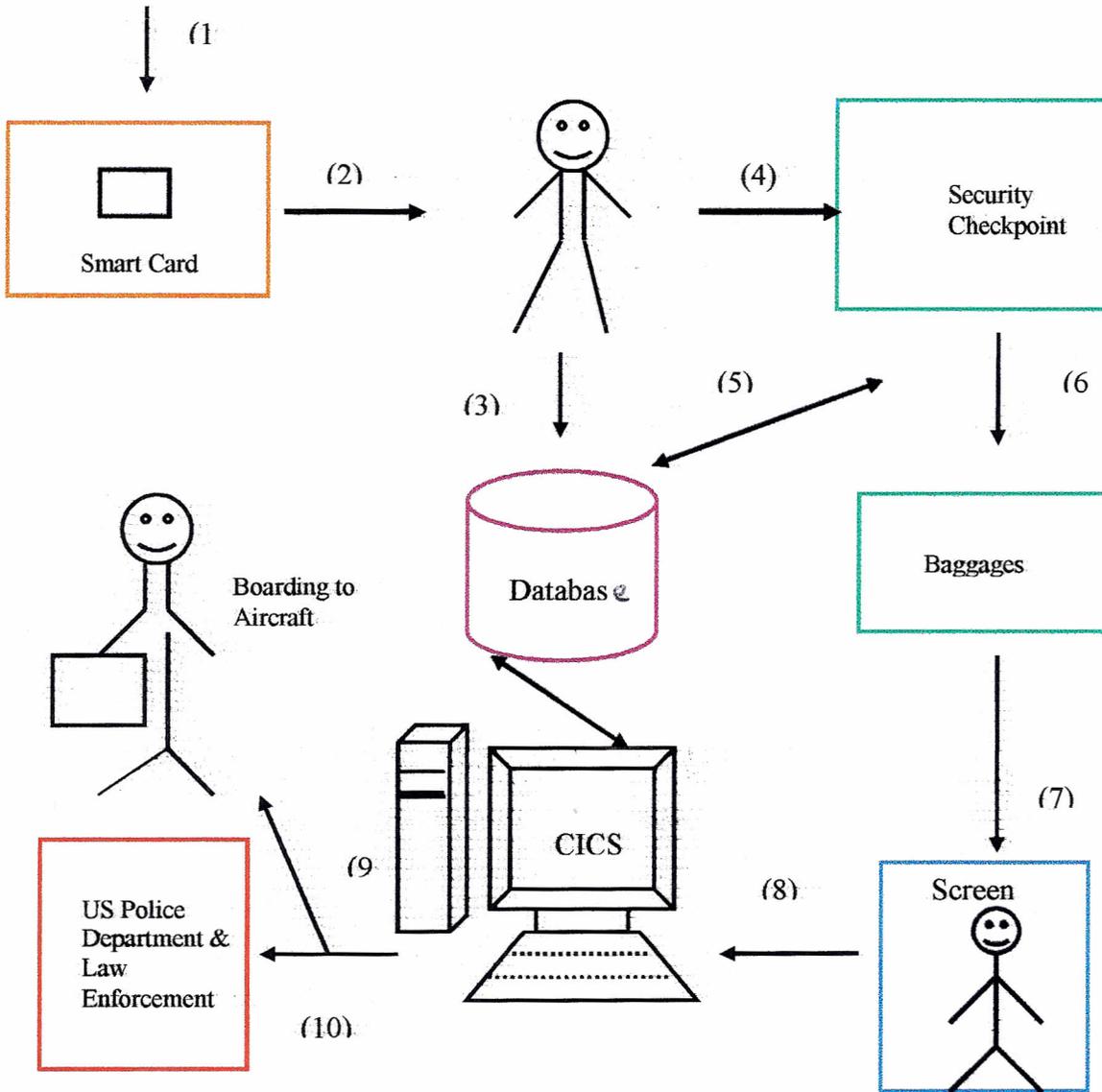
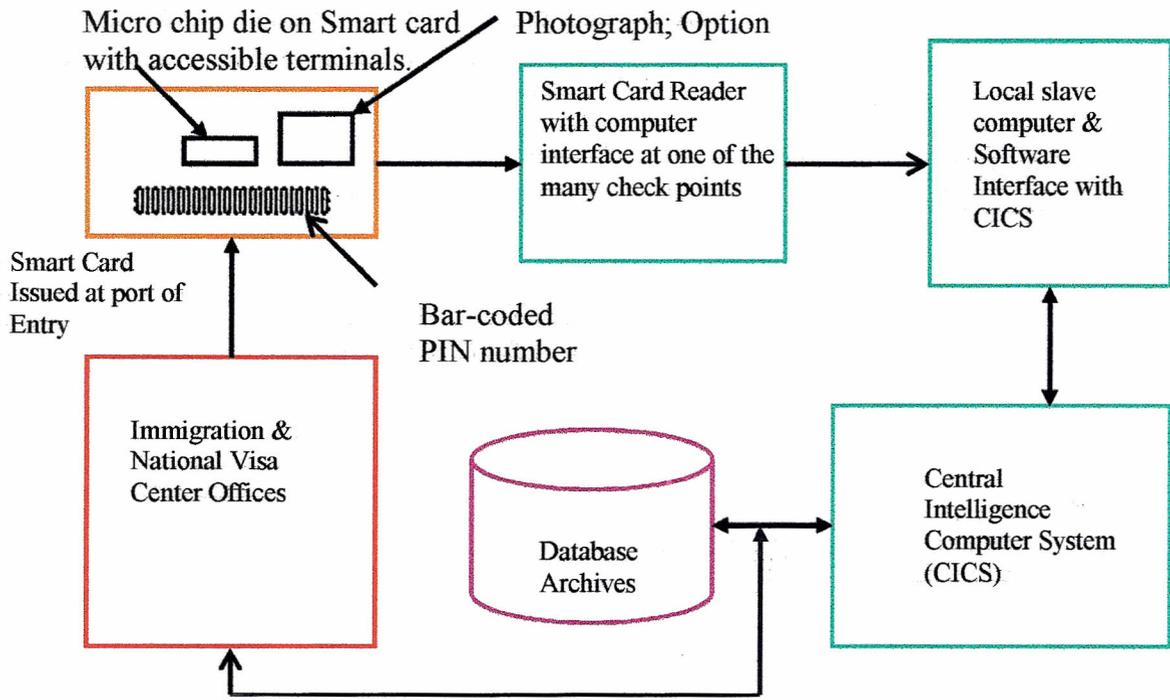


Figure 1. Essential components of the Smart Card System



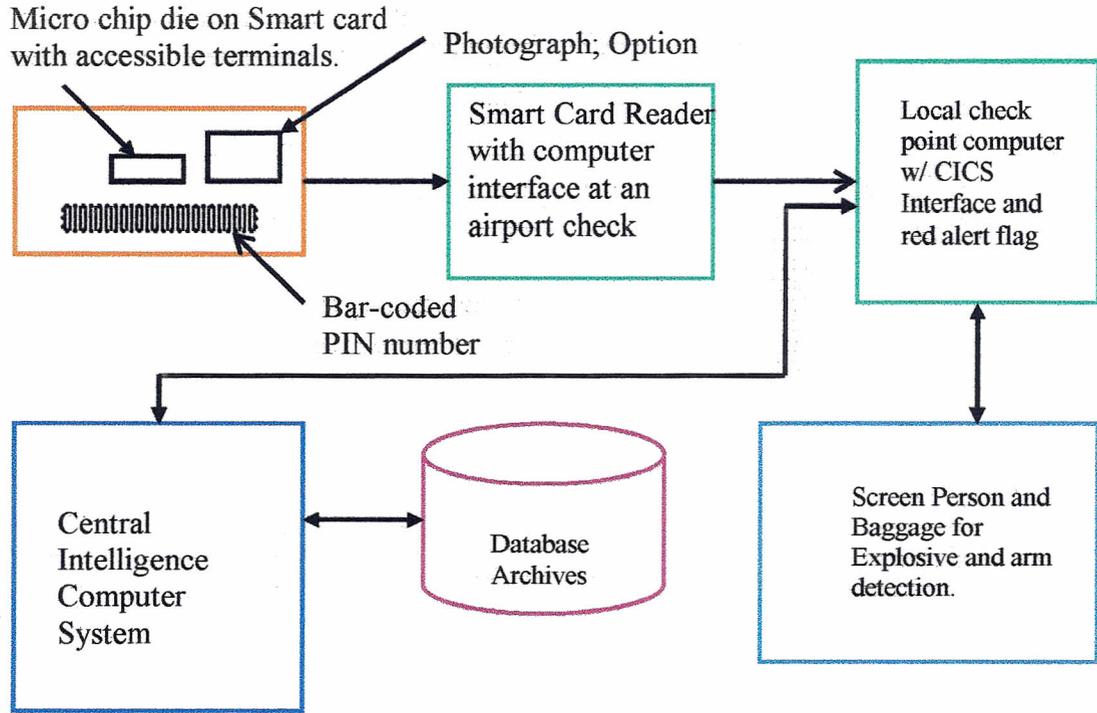
(Proprietary Information)

Figure 1. A pictorial representation of the system



(Proprietary Information)

Figure 2. Smart card system for identity validation.

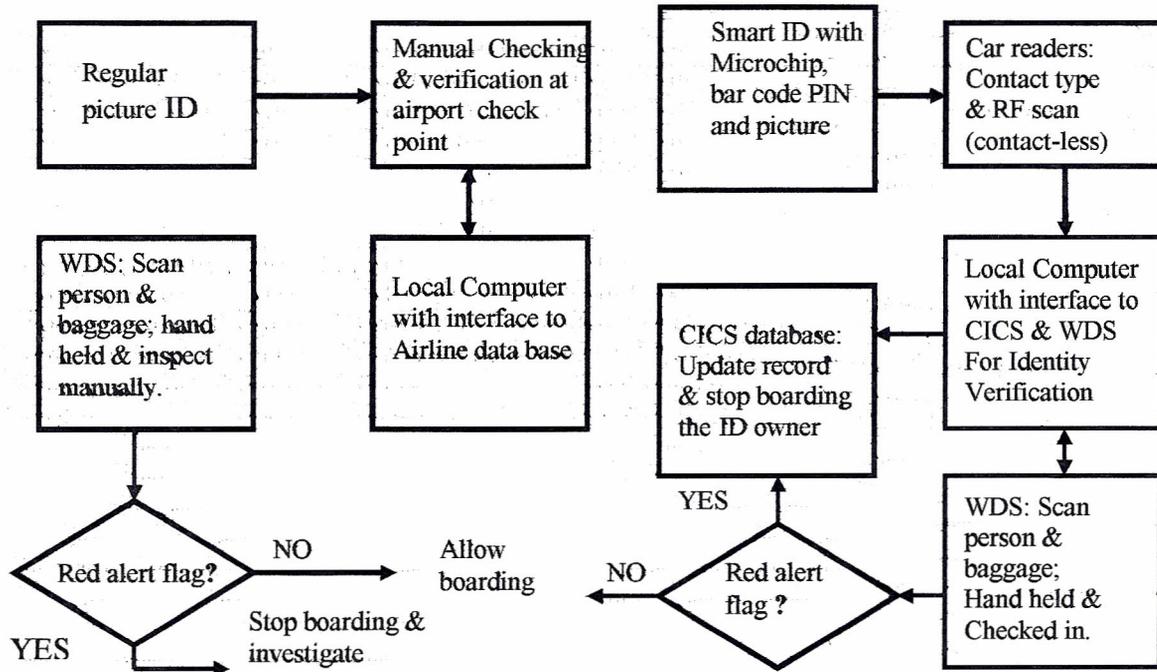


(Proprietary Information)

Figure 3. Smart card system for terror act sensing and prevention.

A. Current State of the Art

B. Our Innovative System



(Proprietary Information)

Figure 4. Conceptual differences between current and new scheme.