



- (51) **International Patent Classification:**
E01F 13/06 (2006.01) *E01F 13/08* (2006.01)
- (21) **International Application Number:**
PCT/IL2024/050692
- (22) **International Filing Date:**
15 July 2024 (15.07.2024)
- (25) **Filing Language:** English
- (26) **Publication Language:** English
- (30) **Priority Data:**
63/534,389 24 August 2023 (24.08.2023) US
- (72) **Inventors; and**
- (71) **Applicants: VARDI, Meir** [IL/IL]; 7 HaHil St., 7687000 Netaim (IL). **NIR, Ziv** [IL/IL]; 13 Hartglass St., 6997120 Tel Aviv (IL).
- (74) **Agent: BRESSLER, Eyal** et al.; DR. EYAL BRESSLER & CO., 1 Rabin Rd., 4925110 Petah Tikva (IL).
- (81) **Designated States** (*unless otherwise indicated, for every kind of national protection available*): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CV, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IQ, IR, IS, IT, JM, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, MG, MK, MN, MU, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, WS, ZA, ZM, ZW.
- (84) **Designated States** (*unless otherwise indicated, for every kind of regional protection available*): ARIPO (BW, CV, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SC, SD, SL, ST,

(54) **Title:** AUTOMATIC, CAR-BY-CAR PASS, HIGH-RESISTANCE BARRIER SYSTEM

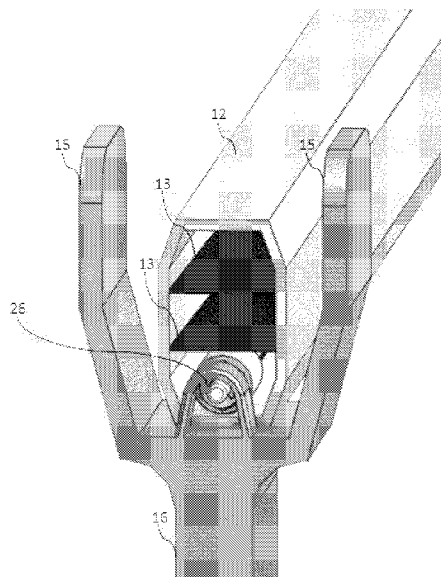


Fig. 3

(57) **Abstract:** A system and method providing an autonomous security system, positioned within a stand configured as a kiosk, for allowing access of unauthorized subjects to an unmanned protected area (UPA) via a checkpoint with a boom barrier. The autonomous security system comprises an electromechanical locking device (ELD) positioned at end of the barrier, steel strip(s) along the barrier for extra physical strength, camera, electro-optical sensor(s) (EOS) and a "fast-gate" mechanism for a "one-car pass". The system further comprises a personal data reader interface configured for collecting personal data selected from: fingerprint scanner, ID card, driving license scanner, a facial camera, and a vehicle plate numbers camera. The personal data is processed and stored in a data storage module, connected to a central control unit (CCU), interconnecting with a barrier control program for opening of the checkpoint boom barrier and a user-controlled module. The user-controlled module is configured to manage and access the data storage module, to delete

SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, RU, TJ, TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, ME, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

Declarations under Rule 4.17:

— *as to applicant's entitlement to apply for and be granted a patent (Rule 4.17(ii))*

Published:

— *with international search report (Art. 21(3))*

the data storage module after a predetermined interval from personal data storage, and to report and transfer the personal data to law authorities center, via a secured connection, if required due to a security breach, or a predetermined signal in a security sensor, during the predetermined time. Furthermore, the CCU is operably connected to a phone call center, allowing validation of authorized subjects to enter the UPA.

AUTOMATIC, CAR-BY-CAR PASS, HIGH-RESISTANCE BARRIER SYSTEM**FIELD OF THE INVENTION**

[001] The present invention is in the field of automatic security systems, particularly kiosk security systems at unmanned protected areas (UPAs).

BACKGROUND OF THE INVENTION

[002] Criminal activities or vandalism might take place within sites that on one hand should be kept open to the public and on the other hand might be attracted to criminal activities (days or nights) like closed gated communities, camping areas, or self-storage facilities. This is a complex challenge that demands a tailored approach to security. To effectively combat the diverse criminal challenges in these sites, a multi-faceted strategy is imperative. By tailoring security solutions to the specific needs of these kinds of sites, it becomes possible to create safer environments that deter criminal activities, enhance response times, and ultimately ensure the security and peace of mind of all stakeholders involved.

[003] First and foremost, security barrier systems currently available on the market do not provide the impenetrable protection consumers are seeking in terms of strength and/or selectivity ("one car pass"). For instance, many barriers may be made from aluminum or wood materials, which are light but easy to break, and are attached only on one side. Additionally, in other cases heavy sliding gates are too slow in closing, allowing "tailgating", means enabling any vehicle to access the protected area without a record or control. Uncontrolled access may also occur when the interval between opening and closing the security barrier is too long,

[004] Furthermore, ineffectiveness of existing security barrier systems derives from heavy reliance on human gatekeepers safeguarding such sites, which is not always possible due to budget limitations or other constraints. Human gatekeepers are susceptible to fatigue, distraction, and lapses in attention, which can compromise the effectiveness of security protocols. Additionally, human error and inconsistent performance can lead to gaps in surveillance, leaving areas vulnerable to unauthorized access and security breaches. Moreover, the need for continuous staffing incurs significant operational costs and logistical challenges. In contrast, the deployment of automated security systems offers a compelling solution to these

shortcomings. With their ability to operate tirelessly and without distraction, automated systems ensure round-the-clock vigilance.

[005] US9659421B2 discloses systems and methods for remotely controlling access of vehicles into and out of a secured area. However, this method refers to at least two kiosks, wherein a first kiosk is positioned at a point of entry and a second kiosk is positioned at a point of exit. Data is stored in a remote operation center and while a vehicle is inside the secured area, the information is verified at the operations center to ensure a sufficient match with identifying information for the vehicle previously stored, before the operation center transmits a signal allowing the vehicle to exit. Thus, the systems and methods disclosed in US9659421, are configured for matching entry and exit data of the vehicle and/or driver.

[006] US8620487B2 discloses vehicle screening methods and systems utilizing one or more biometric identifiers input by or obtained from the vehicle occupant, selected from: biometric data, a barcode, and a unique identification number. The input data provided by the user is compared to a database, thereby permitting the vehicle occupant to be remotely screened and verified before entering into a secure facility based on the biometric identifier(s). The methods and systems disclosed in US8620487B2 enable the entry of only authorized drivers to a secured area, and require the comparison of a driver's biometric data to a pre-existed database of authorized subjects.

[007] There is an unmet need for new autonomous security systems and methods that offer a cost-effective, efficient, and reliable approach to safeguarding populated areas, minimizing human error, maximizing gate strength and selectivity, delivering a higher degree of security assurance, while still allowing a free gate crossing for unauthorized drivers at statutory roads, concomitantly with keeping their privacy.

SUMMARY OF THE INVENTION

[008] The invention described herein encompasses autonomous security systems and methods configured for allowing controlled access of unauthorized subjects and preventing access of other unauthorized subjects to an unmanned protected area (UPA).

[009] According to a first aspect, there is provided an autonomous security system, positioned within a stand configured as a kiosk, for allowing controlled access of an unauthorized subject to an unmanned protected area (UPA) via a checkpoint, characterized by:

- a. a security barrier apparatus, comprising:
 - i. a first elongate structural member configured to prevent access into the UPA and disposed in a horizontal plane when in a closed position; the first elongate structural member comprises at least one strip or cable of steel embedded along its length;
 - ii. a first upright member permanently coupled to a first end of the elongate structural member;
 - iii. a second upright member configured to snare the first elongate structural member when pivoted into the closed position, comprising two horns extending substantially vertically from the second upright member, adjacent to a second end of the first elongate structural member in a direction orthogonal to a length axis of the first elongate structural member;
 - iv. an electromechanical motor coupled to a gear box configured to rotate the first elongate structural member between closed and open positions; and
 - v. a power source configured to supply an electrical current to the electric motor;
 - vi. an electro-optical sensor (EOS) configured to detect, track and identify completion of passage of the subject to the UPA;wherein the security barrier apparatus comprises an electromechanical locking device (ELD) mounted on or in the security barrier apparatus locking the first elongate structural member to the second upright member;
- b. a personal data reader interface comprising at least one scanner, at least one camera, and both, for reading and recording all relevant personal data of the subject;
- c. a data storage module, configured to store the personal data, comprising a software timestamp generator that generates timestamps associated with each set of captured personal data; and
- d. a central control unit (CCU) operably connected with the personal data reader interface, with the data storage module and with the checkpoint gate, the CCU

comprising:

- i. one or more processors;
- ii. a program for processing the personal data;
- ii. a barrier control program configured to:
 - 1) open the security barrier apparatus after completion of processing and storing the personal data; and
 - 2) close the security barrier apparatus within a minimum time frame after passage of the subject to the UPA; and
- iii. a user-controlled module configured to receive the personal data from the personal data storage module, further configured to instruct deletion of the stored personal data on receiving a deletion user command;

wherein the user-controlled module is further configured to report and transfer, whenever required, the stored personal data to a control center of law enforcement authorities on receiving a reporting user command, via a secured connection, for identification of an unauthorized subject suspicious in an unusual activity in the UPA.

[010] In some embodiments, the ELD comprises:

- a. a power source configured to supply an electrical current to the ELD;
- b. a first group of electrically conductive wires embedded in the first elongate structural member configured to couple the ELD to the power source; and
- c. a second group of electrically conductive wires embedded in the first elongate structural member configured to couple the ELD to the CCU for "Lock"/"Unlock" commands and indications.

[011] In some embodiments, the barrier control program is configured to enable only one subject at a time to access the UPA during opening/closing of the security barrier apparatus.

[012] In some embodiments, the security barrier apparatus further comprises a counterweight configured to balance the opening/closing.

[013] In some embodiments, the gear box is configured to rotate the first elongate structural member in a vertical arc to a near vertical position when opened.

[014] In some embodiments, the CCU comprises a settings module with adjustable parameters; the adjustable parameters selected from the group consisting of an opening/closing speed adjustment, an opening/closing slowdown feature, and a standard time clock function.

[015] In some embodiments, the at least one strip or cable of steel comprises at least two strips or cables of steel.

[016] In some embodiments, the at least two strips or cables of steel comprises a plurality of strips or cables of steel.

[017] In some embodiments, the first elongate structural member is made from aluminum.

[018] In some embodiments, the security barrier apparatus can be fitted with a lower skirt or an upper hi-bar.

[019] In some embodiments, deletion of the stored personal data is automatically initiated after a predetermined interval between storing the personal data and a positive report of no unusual suspicious activity.

[020] In some embodiments, deletion of the stored personal data is automatically initiated after a predetermined interval between storing the personal data and no report on unusual suspicious activity.

[021] In some embodiments, a predetermined interval is about 24 hrs.

[022] In some embodiments, the autonomous security system further comprising a security sensor interconnected to the user-controlled module, wherein the unusual suspicious activity activates a predetermined signal in the security sensor.

[023] In some embodiments, the security sensor is further operably connected to a control center of law enforcement authorities, and reporting and transferring the stored personal data to the control center is automatically triggered by the predetermined signal from the security sensor.

[024] In some embodiments, the data storage module comprises a personal database of authorized subjects to enter the UPA, further wherein the central control unit comprises a program configured to compare between the subject personal data and the personal database, further wherein an unauthorized subject is determined by the absence of a predetermined match between the subject personal data and the personal database.

[025] In some embodiments, the CCU is interconnected to a phone call center and comprises phone numbers database of authorized subjects to enter the UPA, further wherein opening of the checkpoint gate is after subject's phone number validation by the phone call center, or after completion of processing and storing the personal data.

[026] In some embodiments, the subject is a driver, and the checkpoint is a vehicle entrance gate.

[027] In some embodiments, the autonomous security system comprising an autonomous license plate recognition (ALPR) system, configured to capture and record the vehicle license plate numbers, and operably connected to the central control unit, wherein:

- a. the vehicle license plate numbers are recognized by the ALPR system, the driver is recognized as an authorized driver and the vehicle entrance gate is opened; and
- b. the vehicle license plate numbers are not recognized by the ALPR system, the driver is recognized as an unauthorized driver and the vehicle entrance gate is opened after a notification from the data storage module that the personal data was stored.

[028] In some embodiments, the personal data reader interface comprises at least one component selected from the group consisting of:

- a. a fingerprint scanner;
- b. an ID card or Driving License scanner;
- c. a facial camera; and
- d. a vehicle plate numbers camera.

[029] In some embodiments, the autonomous security system further comprising a sign positioned near the kiosk, providing instructions to drivers on the verification process.

[030] According to another aspect there is provided a method for allowing access of an unauthorized subject to a UPA via a checkpoint, the method comprising steps of:

- a. placing the autonomous security system disclosed herein, adjacent to a checkpoint of the UPA;
- b. instructing an authorized subject to be identified for entering the UPA;
- c. instructing an unauthorized subject to provide personal data by the autonomous security system; once personal data storage is completed, the checkpoint gate is

opened;

- d. sending an "Unlock" command to the ELD by the CCU;
- e. sending an "Open" indication to the CCU by the ELD;
- f. sending an "Open" command to the electromechanical motor by the CCU;
- g. sending an "Open" indication from the electromechanical motor to the CCU;
- h. sending a "Car-passing" indication to the CCU by an EOS;
- i. sending a "Clear" indication to the CCU by the EOS;
- j. sending a "Close" command to an electromechanical motor by the CCU;
- k. sending a "Close" indication from the electromechanical motor to the CCU;
- l. sending a "Lock" command to the ELD by the CCU;
- m. sending a "Lock" indication to the CCU by the ELD;
- n. automatically recording time from the personal data storage:
 - i. if a security breach is reported, the user-controlled module can be accessed by the user, the stored personal can be reported and transferred by the user to a control center of law enforcement authorities, via a secured connection, by providing a user command, for identification of an unauthorized subject suspicious in an unusual activity in the UPA; and
 - ii. if there is no unusual activity in the UPA during a predetermined interval from the personal data storage, the stored personal data is automatically deleted.

[031] In some embodiments, step (b) of providing personal data by an unauthorized subject comprises the steps of:

- a. selecting the personal data reader program selected from: fingerprint scanning, facial recognition, or ID card or Driving License scanning;
- b. for fingerprint scanning, placing the hand on designated scanning area; for facial recognition, positioning the face within the marked area or aligning it with the camera; for ID card or Driving License scanning, placing the ID card or Driving License on designated scanning area; and
- c. receiving a notification that the personal data is valid and recorded.

[032] In some embodiments, reporting and transferring the stored personal data to a control center of law enforcement authorities is automatically triggered by the predetermined signal from the security sensor.

[033] In some embodiments, the method comprising after the step (a) and before the step (b), a step of distinguishing between the authorized subject and the unauthorized subject.

[034] In some embodiments, the step of distinguishing comprises instructing the subject to provide personal data, further wherein a positive notification indicates that the subject is authorized to access the UPA based on the personal database of authorized subjects.

[035] In some embodiments, the step of distinguishing comprises instructing the subject to provide their phone number, further wherein a positive notification indicates that the subject is authorized to access the UPA based on the phone numbers database of authorized subjects.

[036] In some embodiments, the method is configured to allow access of an unauthorized driver to a UPA via a vehicle entrance gate.

[037] In some embodiments, instructing an authorized subject to be identified for entering the UPA in step (b) is by an ALPR system.

[038] In some embodiments, the dimensions, the cameras, and the sensors of the kiosk are adjustable to a driver within a vehicle, allowing collecting the personal data without the need of stepping out of the vehicle.

[039] Unless otherwise defined, all technical and/or scientific terms used herein have the same meaning as commonly understood by one of ordinary skill in the art to which the invention pertains. Although methods and materials similar or equivalent to those described herein can be used in the practice or testing of embodiments of the invention, exemplary methods and/or materials are described below. In case of conflict, the patent specification, including definitions, will control. In addition, the materials, methods, and examples are illustrative only and are not intended to be necessarily limiting.

[040] Further embodiments and the full scope of applicability of the present invention will become apparent from the detailed description given hereinafter. However, it should be understood that the detailed description and specific examples, while indicating preferred embodiments of the invention, are given by way of illustration only, since various changes and modifications within the spirit and scope of the invention will become apparent to those skilled in the art from this detailed description.

BRIEF DESCRIPTION OF THE DRAWINGS

[041] The present invention will be understood and appreciated more fully from the following detailed description taken in conjunction with the figures in which:

[042] **Figure 1** is a simplified diagrammatic view illustrating the components of the autonomous security system for allowing access of a subject to an unmanned protected area (UPA) via a checkpoint, in accordance with an embodiment of the present disclosure.

[043] **Figure 2** is an illustration showing the components of the autonomous security system, positioned within a stand configured as a kiosk, and method thereof, for allowing access of an unauthorized subject to an unmanned protected area (UPA) via a checkpoint, in accordance with an embodiment of the present disclosure.

[044] **Figure 3** is an illustration showing the components of the first elongate structural member and second upright member of the security barrier apparatus, including the electromagnetic locking device (ELD), in accordance with an embodiment of the present disclosure.

[045] **Figure 4** is a is an illustration showing the components of the security barrier apparatus, in accordance with an embodiment of the present disclosure.

[046] **Figure 5** is a simplified high-level flowchart illustrating the components of the autonomous security system for allowing access of a subject to an unmanned protected area (UPA) via a checkpoint, in accordance with an embodiment of the present disclosure.

[047] **Figure 6** is a simplified high-level flowchart illustrating the steps involved in the method for allowing access of a subject to an unmanned protected area (UPA) via a checkpoint, in accordance with an embodiment of the present disclosure.

[048] **Figure 7** is a simplified high-level flowchart illustrating the steps involved in the method for allowing access of a subject to an unmanned protected area (UPA) via a checkpoint, in accordance with an embodiment of the present disclosure.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

[049] The presently disclosed subject matter may be more clearly understood upon reading of the following detailed description embodiments of non-limiting exemplary embodiments thereof, with reference to the drawings.

[050] The following detailed description of embodiments of the presently disclosed subject matter refers to accompanying drawings. Dimensions of components and features shown in figures are chosen for convenience or clarity of presentation and are not necessarily shown to scale. Wherever possible, the same reference numbers will be used throughout the drawings and the following description to refer to the same and like parts.

Autonomous Security System

[051] According to a first aspect, there is provided an autonomous security system, positioned within a stand configured as a kiosk, for allowing access of an unauthorized subject to an unmanned protected area (UPA) via a checkpoint. In some embodiments, the autonomous security kiosk system is configured to deter a suspicious subject from entering the UPA. In some embodiments the kiosk is located near a checkpoint. In some embodiments, the subject is a driver. In some embodiments, the kiosk is positioned on a statutory road. In some embodiments, the checkpoint is a vehicle entrance gate.

[052] The autonomous security kiosk system disclosed herein is configured to allow access of an unauthorized subject to a UPA, only after the subject provides valid personal data. In some embodiments, the autonomous security kiosk system allows access of an unauthorized subject during closed hours of an entry gate. The autonomous security kiosk system is designated to securely save the recorded personal data for a predetermined time. If during the predetermined time a security breach (e.g., a burglary or a theft incident) occurs, the user can transfer the collected personal data to a legal authorities' center, for investigation purposes (e.g., identification of potential suspects). If there is no report of a security breach during the predetermined time, the recorded personal data is automatically erased. Securing the saved personal data and its transmission to legal authorities, and erasing this data after the predetermined time, allows the access of unauthorized subjects to a secured area, while avoiding the violation of human rights to privacy.

[053] As used herein, the term "**unmanned protected area (UPA)**" refers to a place that requires implementation of security measures to safeguard against unauthorized access, theft, and other potential risks. Examples for such secured areas include: closed gated community, camping areas, factories, and self-storage facilities. In some embodiments, UPA is any self-protected area that should be opened to the public. The term "**statutory road**" disclosed herein encompasses a road that requires authorization for access.

[054] In some embodiments, the autonomous security system comprises:

- a. a security barrier apparatus, comprising:
 - i. a first elongate structural member configured to prevent access into the UPA and disposed in a horizontal plane when in a closed position; the first elongate structural member comprises at least one strip or cable of steel embedded along its length;
 - ii. a first upright member permanently coupled to a first end of the elongate structural member;
 - iii. a second upright member configured to snare the first elongate structural member when pivoted into the closed position, comprising two horns extending substantially vertically from the second upright member, adjacent to a second end of the first elongate structural member in a direction orthogonal to a length axis of the first elongate structural member;
 - iv. an electromechanical motor coupled to a gear box configured to rotate the first elongate structural member between closed and open positions; and
 - v. a power source configured to supply an electrical current to the electric motor;
 - vi. an electro-optical sensor (EOS) configured to detect, track and identify completion of passage of the subject to the UPA;wherein the security barrier apparatus comprises an electromechanical locking device (ELD) mounted on or in the security barrier apparatus locking the first elongate structural member to the second upright member;
- b. a personal data reader interface comprising at least one scanner, at least one camera, and both, for reading a subject personal data;
- c. a data storage module, configured to store the personal data, comprising a software timestamp generator that generates timestamps associated with each set of captured personal data; and
- d. a central control unit operably connected with the personal data reader, with the data storage module and with the checkpoint gate, the central control unit comprising:
 - i. one or more processors;
 - ii. a program for processing the personal data;

- ii. a barrier control program, configured to:
 - 1) open the security barrier apparatus after completion of processing and identification of an authorized subjects; and
 - 2) open the security barrier apparatus after completion of processing and storing the personal data of unauthorized subjects;
 - 3) close the security barrier apparatus within a minimum time frame after passage of the subject to the UPA in order to prevent more than one subject pass at a time; and
 - 4) close the security barrier apparatus within a predefined time frame if a passage of a subject to the UPA is not detected; and
- iii. a user-controlled module configured to receive the personal data from the personal data storage module.

[055] In some embodiments, the user-controlled module is configured to instruct deletion of the stored personal data on receiving a deletion user command.

[056] The term "**deletion user command**" used herein refers to a command to delete the personal data after either on a user command or after a predetermined time from which it was recorded.

[057] In some embodiments, the user-controlled module is configured to report and transfer the stored personal data to a control center of law enforcement authorities on receiving a reporting user command, for identification of an unauthorized subject suspicious in an unusual activity in the UPA. In some embodiments, reporting and transferring the stored personal data is by a secured connection. In some embodiments, the connection is wired connection or wireless connection.

[058] The term "**reporting user command**" refers to a command to report and transfer the personal data to a control center of law enforcement authorities. In some embodiments, the user can instruct the reporting window time (i.e., the personal data between two time points defined by the user).

[059] The term "**minimum time frame**", used herein, is between 1 second and 10 seconds. In some embodiments, the "**minimum time frame**" is between 1.5 seconds and 8 seconds. In some embodiments, the predetermined interval is about 3 seconds. In some embodiments, the "**minimum time frame**" is adjustable through the CCU. The "**minimum time frame**" enables a "fast" mechanism of the autonomous security system disclosed herein, facilitating a "one-car

pass", i.e., only one subject at a time may access the UPA during opening/closing of the security barrier apparatus.

[060] In some embodiments, the gearbox disclosed herein is configured to enable slow raising and fast lowering of the first elongate structural member to prevent "tailgating". In some embodiments, the counterweight disclosed herein is configured to balance the opening/closing of the first elongate structural member.

[061] As used herein, a "**personal data reader interface**" refers to hardware and software components essential for capturing the subject personal data accurately. A personal data reader interface comprises at least one personal data scanner designed to capture personal features such as fingerprints or an ID card or Driving License, at least one camera designed to capture a high-resolution image of a face of subject.

[062] The term "**data storage module**" refers to hardware and software components that are responsible for storing and managing the captured personal data securely, including: a physical or a digital storage medium (e.g., a cloud server), capable of holding data for a predetermined time; data management software program that handles data storage, ensuring proper organization, secure encryption, and data integrity; and an automated data deletion program that manages data deletion after the predetermined time has elapsed.

[063] Examples for physical storage medium can include: a hard drive; a solid-state drive (SSD); a combination of both hard drive and SSD; and a random-access memory (RAM).

[064] In some embodiments, the data management software includes a software timestamp generator that generates timestamps that are associated with each set of captured data, allowing the system to determine when the data should be deleted.

[065] In some embodiments, the automated data deletion program comprises a script or program that runs within the system, monitoring timestamps and triggering the deletion of data once the predetermined duration has passed.

[066] The automated data deletion program may further comprise a secure deletion mechanism ensuring that data is securely and irreversibly deleted from the storage medium, often by overwriting the data with random values or following established cryptographic methods.

[067] In some embodiments, the automated data deletion program automatically deletes the stored personal data after a predetermined interval between storing the personal data and a positive report of no unusual suspicious activity.

[068] In some embodiments, the automated data deletion program automatically deletes the stored personal data after a predetermined interval between storing the personal data and no report on unusual suspicious activity.

[069] It is noted that the term "**user**", used herein, refers to an individual that operates the autonomous security system disclosed herein. The term "**subject**" is used herein to describe an individual aiming to enter the UPA. The term "**personal data**" is used herein to describe any data that can be obtained from a subject and is used for subject identification purposes. In some embodiments, personal data comprises biometric data. In some embodiments, personal data is selected from: fingerprints picture, ID picture, Driving License picture, subject's face picture, subject's vehicle license plate picture, and subject's phone number.

[070] In some embodiments, the predetermined interval is between 8 hrs and 1 week. In some embodiments, the predetermined interval is between 16 hrs and 72 hrs. In some embodiments, the predetermined interval is about 24 hr.

[071] In some embodiments, the data storage module comprises physical and/or software mechanisms that control who can access the stored data. These mechanisms could involve physical security measures for the storage device and software-based access controls. Examples for software-based access controls include: role-based access control (RBAC), granting different levels of access based on user roles and responsibilities; multi-factor authentication (MFA), such as a password and a unique code sent to the user mobile device; time-based access software that restricts access to specific time periods, ensuring that only authorized personnel can access data during designated times; audit trails allowing administrators to track user activity; encryption of the stored data within the software both at rest and during transmission; IP whitelisting, allowing only specific IP addresses or ranges to access the software; intrusion detection system (IDS) that detects and alerts administrators about suspicious activities, unauthorized access attempts, or unusual patterns; and account lockout software which locks a user's account, after a specified number of failed login attempts.

[072] In some embodiments, the data storage module further comprises audit logging software that keeps track of all data storage and deletion activities for auditing purposes.

[073] In some embodiments, the **"user-controlled module"** disclosed herein comprises secured communication protocols and hardware to facilitate data transmission to a control center of law authorities, ensuring secure and reliable transfer.

[074] In some embodiments, the user-controlled module comprises an authentication mechanism ensuring that the user is authenticated before allowing data retrieval and reporting actions to maintain security. In some embodiments, the user-controlled module comprises encryption and security measures to protect the data during transmission and storage.

[075] In some embodiments, the user-controlled module is operably connected to a security sensor in the UPA, and an unusual suspicious activity activates a predetermined signal in the security sensor. In some embodiments, the user is promptly notified of a security breach by the disclosed security system. The user is then able to actively report and transfer the stored personal data when necessary.

[076] Security sensors that detect movement within a designated area are known in the art. Non-limiting examples for such security sensors include: a motion sensor that detects movement, intrusion detection sensors, including door/window contact sensors, glass break detectors, or vibration sensors, break beam sensors that use a laser or infrared beam between two points, activating an alarm when the beam is interrupted, a sound detection sensors, a temperature and smoke sensors indicating potential fire or other hazards, a pressure mat sensor that is placed on the ground and detects pressure changes when someone steps on it, a video analytics sensor detecting specific patterns such as loitering, proximity sensors detecting the presence of an object or person within a certain range.

[077] In some embodiments, the security sensor is further operably connected to a control center of law enforcement authorities, and the reporting and transferring the stored personal data to the control center is automatically triggered by the predetermined signal from the security sensor.

[078] In some embodiments, the autonomous security system further comprises programs and means configured for distinguishing between an authorized subject and an unauthorized subject.

[079] In some embodiments, distinguishing between an authorized subject and an unauthorized subject is based on a positive match with a personal database of predetermined authorized subjects. In some embodiments, the data storage module comprises a personal database of authorized subjects to enter the UPA, and the central control unit comprises a

program configured to compare between the personal data of the subject aiming to enter the UPA, and the personal database. In some embodiments, an authorized subject is determined by the presence of a predetermined match between the subject personal data and the personal database, and an unauthorized subject is determined by the absence of a predetermined match between the subject personal data and the personal database.

[080] The database of personal data in the described kiosk security system can be stored within the internal storage or memory of the secured autonomous security system, as well as potentially on a centralized server or secure cloud storage system, depending on the design and architecture of the system.

[081] In some embodiments, distinguishing between an authorized subject and an unauthorized subject is based on a positive match with a phone numbers database of predetermined authorized subjects. In some embodiments, the central control unit is interconnected to a predetermined phone call center and comprises phone numbers database of authorized subjects to enter the UPA.

[082] In some embodiments, the barrier control program is configured to open the checkpoint gate if one of the following occurs:

- a. a signal from the predetermined phone call center or the central control unit, indicating that the phone number of the calling subject, aiming to enter the UPA, is validated; the subject is identified as an authorized subject;
- b. a signal from the data storage module that the personal data of the subject aiming to enter the UPA matches the personal data in the personal database; the subject is identified as an authorized subject; and
- c. a first signal from the data storage module that the personal data of the subject aiming to enter the UPA does not match the personal data in the personal database; the subject is identified as an unauthorized subject; and a second signal from the data storage module that the subject's personal data is recorded.

[083] In some embodiments, an authorized subject can call the dedicated phone number from their registered phone, prior approaching the checkpoint, and an automated voice system may guide the subject through the authentication process. In some embodiments, if the provided

phone number matches an authorized subject, the system either automatically open the checkpoint gate, or provides a one-time access code that the subject is required to enter using their phone's keypad.

[084] In some embodiments, the subject is a driver. In some embodiments, the checkpoint is a vehicle entrance gate.

[085] In some embodiments, the autonomous security system comprises an automatic license plate recognition (ALPR) system, configured to capture and record the vehicle license plate numbers, and operably connected to the central control unit.

[086] In some embodiments, the barrier control program is configured to open the checkpoint gate if one of the following occurs:

- a. a signal from an ALPR system, indicating that the vehicle license plate numbers are validated; the subject is identified as an authorized subject;
- b. a signal from the predetermined phone call center, indicating that the phone number of the subject aiming to enter the UPA is validated; the subject is identified as an authorized subject;
- c. a signal from the data storage module that the personal data of the subject aiming to enter the UPA matches the personal data in the personal database; the subject is identified as an authorized subject; and
- d. a first signal from the data storage module that the personal data of the subject aiming to enter the UPA does not match the personal data in the personal database; the subject is identified as an unauthorized subject; and a second signal from the data storage module that the subject's personal data is recorded.

[087] As used herein, the term "**automatic license plate recognition (ALPR) system**", and "**automatic number plate recognition (ANPR)**", are interchangeably used, and encompass a technology that uses optical character recognition to automatically read license plates on vehicles. The ALPR system typically comprises high-resolution cameras, an illumination source (e.g., infrared or white light illuminators, an image processing software; an optical character recognition (OCR) algorithm identifying and decoding characters on the license plate, database and search engine for storing and indexing license plate data, and network connectivity to transmit data between cameras, processing software, and databases.

[088] In some embodiments, the personal data reader interface comprises at least one component selected from the group consisting of:

- a. a fingerprint scanner;
- b. an ID card or Driving License card scanner;
- c. a facial camera; and
- d. a vehicle plate numbers camera.

[089] As used herein, the term "**fingerprint scanner**", refers to a device that captures a fingerprint pattern for authentication and identification purposes. The components of a fingerprint scanner can include: a sensor responsible for capturing the fingerprint image (e.g., optical, capacitive, and ultrasonic sensors), light source for optical sensors to illuminate the fingerprint, capacitive array for capacitive sensors to detect the electrical differences between ridges and valleys on a fingerprint, an ultrasonic transducer for ultrasonic sensors to capture the unique 3D features of a fingerprint, an image processing software, drivers and software development kit (SDKs) that enable integration into various applications and systems, such as security software or access control systems, and optimally LED indicators and feedback that provide feedback to the subject about the scanning process, successful recognition, or any errors.

[090] As used herein, the term "**ID card or Driving License scanner**" refers to a device used to capture information from identification cards, such as ID card or Driving Licenses, and passports. An ID card or Driving License scanner can include an optical sensor, an illuminating light source, an image processing software, an OCR algorithm, and optionally; a magnetic stripe reader, a smart card reader that allows the scanner to interact with the card's embedded microchip, and a barcode scanner.

[091] The used herein, the terms "facial camera" and "**facial recognition camera**" are interchangeably used and refer to a high-resolution camera, designed to capture and analyze facial features for identification and authentication purposes. The main components of a facial recognition camera include: a camera module, a high-quality lens system, infrared illumination for low-light or nighttime scenarios, an image processing software, and a facial recognition algorithm that analyzes facial features, identifies key points (landmarks), and creates a facial template.

[092] In some embodiments, a sign providing instructions to drivers on the verification process, is positioned near the kiosk.

[093] In some embodiments, high visibility "stop" or "no entry" signs and a LED light array may be specified to the first elongate structural member of the security barrier apparatus.

[094] The autonomous security kiosk system disclosed herein may be retrofitted in existing security systems limiting access into UPAs. Retrofitting the disclosed security system provides an easy-installation and cost-effective solution to gate entry systems for improved security and convenience.

Methods of Using the Autonomous Security System

[095] According to another aspect, there is provided a method for allowing access of an unauthorized subject to an unmanned protected area (UPA) via a checkpoint, the method comprising steps of:

- a. placing the autonomous security system disclosed herein, adjacent to a checkpoint of UPA;
- b. instructing an authorized subject to be identified for entering the UPA;
- c. instructing an unauthorized subject to provide personal data by the autonomous security system; once personal data storage is completed, the checkpoint gate is opened; and
- d. sending an "Unlock" command to the electromechanical locking device (ELD) by the central control unit (CCU);
- e. sending an "Open" indication to the CCU by the ELD;
- f. sending an "Open" command to the electromechanical motor by the CCU;
- g. sending an "Open" indication from the electromechanical motor to the CCU;
- h. sending a "Car-passing" indication to the CCU by an electro-optical sensor (EOS);
- i. sending a "Clear" indication to the CCU by the EOS;
- j. sending a "Close" command to an electromechanical motor by the CCU;
- k. sending a "Close" indication from the electromechanical motor to the CCU;
- l. sending a "Lock" command to the ELD by the CCU;

- m. sending a "Lock" indication to the CCU by the ELD;
- n. automatically recording time from the personal data storage:
 - i. if a security breach is reported, the user-controlled module can be accessed and viewed by the user, the stored personal can be reported and transferred by the user to a control center of law enforcement authorities, via a secured connection, by providing a user command, for identification of an unauthorized subject suspicious in an unusual activity in the UPA; and
 - ii. if there is no unusual activity in the UPA during a predetermined interval from the personal data storage, the stored personal data is automatically deleted.

[096] In some embodiments, the step (b) of providing personal data by an unauthorized subject comprises the steps of:

- a. selecting the personal data reader program selected from: fingerprint scanning, facial recognition, or ID card or Driving License scanning;
- b. for fingerprint scanning, placing the hand on the designated scanning area; for facial recognition, positioning the face within the marked area or aligning it with the camera; for ID card or Driving License scanning, placing the ID card or Driving License on designated scanning area; and
- c. receiving a notification that the personal data is valid and recorded.

[097] In some embodiments, reporting and transferring the stored personal data to a control center of law enforcement authorities is automatically triggered by the predetermined signal from the security sensor.

[098] In some embodiments, the method comprising after the step (a) and before the step (b), a step of distinguishing between the authorized subject and the unauthorized subject.

[099] In some embodiments, the step of distinguishing comprises instructing the subject to provide personal data, further wherein a positive notification indicates that the subject is authorized to access the UPA based on the personal database of authorized subjects.

[0100] In some embodiments, the step of distinguishing comprises instructing the subject to provide their phone number, further wherein a positive notification indicates that the subject is authorized to access the UPA based on the phone numbers database of authorized subjects.

[0101] In some embodiments, the method is configured to allow access of an unauthorized driver to a UPA via a vehicle entrance gate. In some embodiments, the instructing an authorized

subject to be identified for entering the UPA in step (b) is by an automatic license plate recognition (ALPR) system, as disclosed herein.

[0102] In some embodiments, the dimensions, the cameras, and the sensors of the kiosk disclosed herein are adjustable to a driver within a vehicle, allowing collecting the personal data without the need of stepping out of the vehicle.

[0103] Reference is now made to Fig. 1, which shows a simplified diagrammatic view of the components of the autonomous security system for allowing access of a subject to a UPA via a checkpoint, in accordance with an embodiment of the present disclosure. The autonomous security system, positioned within a stand configured as a kiosk **10**, comprising a personal data reader interface **19**, and located adjacent to a security barrier apparatus, configured to supervise the access of unauthorized subjects to a UPA. The security barrier apparatus is comprised of a first elongate structural member **12**, a first upright member **14** and a second upright member **16**. The first elongate structural member **12** is configured to rotate in a vertical arc to a near vertical position when opened, thus enabling only one subject **11** at a time to access the UPA during opening/closing of the security barrier apparatus.

[0104] Fig. 2 is an illustration showing the components of the autonomous security system, positioned within a stand configured as a kiosk **10**, comprising a personal data reader interface **19**, for allowing access of an unauthorized subject to a UPA via a checkpoint, in accordance with an embodiment of the present disclosure. The security barrier apparatus is comprised of a first elongate structural member **12**, a first upright member **14** and a second upright member **16**. The first elongate structural member **12** is disposed in a horizontal plane when in a closed position, and rotates in a vertical arc to a near vertical position when opened. The security barrier apparatus enables only one subject **11** at a time to access the UPA during opening/closing of the security barrier apparatus. A second security barrier apparatus, adjacent to the first security barrier apparatus for accessing the UPA, also comprises a first elongate structural member **12**, a first upright member **14** and a second upright member **16**, and is configured to allow exit of a subject from the UPA.

[0105] Fig. 3 is an illustration showing the components of the first elongate structural member **12** and second upright member **16** of the security barrier apparatus, including the ELD **26**, in accordance with an embodiment of the present disclosure. The first elongate structural member **12** comprises at least one strip or cable of steel **13** embedded along its length. The second upright member **16** is configured to snare the first elongate structural member **12** when pivoted

into a closed position, comprising two horns **15** extending substantially vertically from the second upright member **16**, adjacent to a second end of the first elongate structural member **12** in a direction orthogonal to a length axis of the first elongate structural member **12**.

[0106] Fig. 4 is an illustration showing the components of the security barrier apparatus, in accordance with an embodiment of the present disclosure. The security barrier apparatus is comprised of a first elongate structural member **12** configured to rotate in a vertical arc to a near vertical position when opened, a first upright member **14** and a second upright member **16**. The first upright member **14** is permanently coupled to a first end of the elongate structural member **12**, wherein the first elongate structural member **12** is disposed in a horizontal plane when in a closed position. The second upright member **16** is configured to snare the first elongate structural member **12** when pivoted into a closed position, comprising two horns **15** extending substantially vertically from the second upright member **16**, adjacent to a second end of the first elongate structural member **12** in a direction orthogonal to a length axis of the first elongate structural member **12**. An electromechanical motor **18** coupled to a gear box **20** is configured to rotate the first elongate structural member **12** between closed and open positions. Below the electromechanical motor **18** is a low-voltage power source **22** configured to supply an electrical current via an electrically conductive wire **17**. An ELD **26** is mounted on or in the security barrier apparatus locking the first elongate structural member **12** to said second upright member **16**, wherein a first group of electrically conductive wires **38** is embedded in the first elongate structural member **12**, and configured to couple the ELD **26** to the power source **22**. Furthermore, a second group of electrically conductive wires **40** is embedded in the first elongate structural member **12**, and configured to couple the ELD **26** to the power source **22** to the CCU **30** for "Lock"/"Unlock" commands and indications. Located on the second upright member **16**, an EOS **24** is configured to detect, track and identify completion of passage of a subject to the UPA.

[0107] Fig. 5 is an illustration showing a diagram of autonomous security system components. The autonomous security system comprises a personal data reader interface **11** for collecting personal data selected from: fingerprint scanner, ID card or Driving License scanner, a facial camera, and a vehicle plate numbers camera. The personal data is processed and stored in a data storage module **28**. The processor **32** and the data storage module **28** are connected to a CCU **30**, interconnecting with a barrier control program **34** and a user-controlled module **38**. Once the personal data is successfully stored, the barrier control program **34** instructs opening of the security barrier apparatus **21**. The user-controlled module **38** is configured to manage

and access the data storage module **28**, to delete the data storage module **28** after a predetermined interval from personal data storage, and to report and transfer the personal data to a center of law authorities **40**, via a secured connection, if required due to a security breach during the predetermined time. In a further example, the CCU **30** is triggered to automatically report and transfer the stored personal data by a predetermined signal in a security sensor **36**. In a further specific example, the CCU **30** is operably connected to a phone call center **42**, allowing validation of authorized subjects to enter the UPA.

[0108] Fig. 6 is a simplified example flowchart illustrating the steps involved in a method for allowing access of an unauthorized subject to a UPA via a checkpoint, in accordance with an embodiment of the present disclosure. First, the personal data reader interface is initiated by a subject **102**. An authorized subject is instructed to be identified for entering the UPA **104**, whereas an unauthorized subject is instructed to provide personal data **106**. Once the personal data storage is completed, the checkpoint gate is opened by sending an "Unlock" command to the ELD by the central control unit CCU **108**. Then, an "Open" indication is sent to the CCU by the ELD **110**, followed by an "Open" command sent to the electromechanical motor by the CCU **112**, and an "Open" indication sent from the electromechanical motor to the CCU **114**. Following this, a "Car-passing" indication is sent to the CCU by an electro-optical sensor (EOS) **116**, after which a "Clear" indication is sent to the CCU by the EOS **118**. Finally, a "Close" command is sent to an electromechanical motor by the CCU **120**, a "Close" indication is sent from the electromechanical motor to the CCU **122**, and a "Lock" command is sent to the ELD by the CCU **124**. Once locked, a "Lock" indication is sent to the CCU by the ELD **126**, automatically recording time from said personal data storage **128**. If a security breach has occurred, then stored personal data is reported to a control center of law enforcement authorities **130**. However, if no security breach has occurred, then stored personal data is automatically deleted **132**.

[0109] Fig. 7 is a simplified high-level flowchart illustrating the steps involved in the method for allowing access of a subject to a UPA via a checkpoint, in accordance with an embodiment of the present disclosure. When a vehicle approaches the checkpoint **136**, a listed driver calls a predefined phone number **138**. In contrast, when not listed, a driver approaches the kiosk **140**. The driver then provides personal data and a data file is created with date and time, license plate photo, driver face photo, formal identity card or fingerprints **142**. The same requirement of providing personal data and creating a data file is undertaken when the phone number of a

listed driver is not listed. When the phone number of a listed driver is listed, the gate is opened
144.

[0110] As used herein, the term "about" when combined with a value refers to plus and minus 10% of the reference value. For example, a length of about 1000 nanometers (nm) refers to a length of $1000 \text{ nm} \pm 100 \text{ nm}$.

[0111] It is noted that as used herein and in the appended claims, the singular forms "a", "an", and "the" include plural referents unless the context clearly dictates otherwise.

[0112] In those instances where a convention analogous to "at least one of A, B, and C, etc." is used, in general such a construction is intended in the sense one having skill in the art would understand the convention (e.g., "a system having at least one of A, B, and C" would include but not be limited to systems that have A alone, B alone, C alone, A and B together, A and C together, B and C together, and/or A, B, and C together, etc.). It will be further understood by those within the art that virtually any disjunctive word and/or phrase presenting two or more alternative terms, whether in the description, claims, or drawings, should be understood to contemplate the possibilities of including one of the terms, either of the terms, or both terms. For example, the phrase "A or B" will be understood to include the possibilities of "A" or "B" or "A and B."

[0113] It is appreciated that certain features of the invention, which are, for clarity, described in the context of separate embodiments, may also be provided in combination in a single embodiment. Conversely, various features of the invention, which are, for brevity, described in the context of a single embodiment, may also be provided separately or in any suitable sub-combination. All combinations of the embodiments pertaining to the invention are specifically embraced by the present invention and are disclosed herein just as if each and every combination was individually and explicitly disclosed. In addition, all sub-combinations of the various embodiments and elements thereof are also specifically embraced by the present invention and are disclosed herein just as if each and every such sub-combination was individually and explicitly disclosed herein.

[0114] Additional objects, advantages, and novel features of the present invention will become apparent to one ordinarily skilled in the art upon examination.

CLAIMS

1. An autonomous security system, positioned within a stand configured as a kiosk **10**, for allowing access of an unauthorized subject **11** to an unmanned protected area (UPA) via a checkpoint, characterized by:
 - a. a security barrier apparatus **21**, comprising:
 - i. a first elongate structural member **12** configured to prevent access into said UPA and disposed in a horizontal plane when in a closed position; said first elongate structural member comprises at least one strip or cable of steel **13** embedded along its length;
 - ii. a first upright member **14** permanently coupled to a first end of said elongate structural member **12**;
 - iii. a second upright member **16** configured to snare said first elongate structural member **12** when pivoted into said closed position, comprising two horns **15** extending substantially vertically from said second upright member **16**, adjacent to a second end of said first elongate structural member **12** in a direction orthogonal to a length axis of said first elongate structural member **12**;
 - iv. an electromechanical motor **18** coupled to a gear box **20** configured to rotate said first elongate structural member **12** between closed and open positions; and
 - v. a low-voltage power source **22** configured to supply an electrical current to said electric motor **18** via an electrically conductive wire **17**; and
 - vi. an electro-optical sensor (EOS) **24** configured to detect, track and identify completion of passage of said subject to said UPA;wherein said security barrier apparatus comprises an electromechanical locking device (ELD) **26** mounted on or in said security barrier apparatus locking said first elongate structural member **12** to said second upright member **16**;
 - b. a personal data reader interface **19** comprising at least one scanner, at least one camera, or both, configured to collect personal data of said subject;
 - c. a data storage module **28** configured to store said personal data, comprising a software timestamp generator that generates timestamps associated with each set of

- captured personal data; and
- d. a central control unit (CCU) **30** operably connected with said personal data reader, with said data storage module **28** and with said checkpoint gate, comprising:
- i. one or more processors **32**;
 - ii. a program for processing said personal data;
 - iii. a barrier control program **34** configured to:
 - 1) open said security barrier apparatus after completion of processing and storing said personal data; and
 - 2) close said security barrier apparatus within a minimum time frame after passage of said subject to said UPA; and
 - iv. a user-controlled module **36** configured to receive said personal data from said personal data storage module **28** and instruct deletion of said stored personal data on receiving a deletion user command.
2. The autonomous security system of claim 1, wherein said ELD comprises:
- a. a power source **22** further configured to supply an electrical current to said ELD **26**;
 - b. a first group of electrically conductive wires **38** embedded in said first elongate structural member **12** configured to couple said ELD **26** to said power source **22**;
and
 - c. a second group of electrically conductive wires **40** embedded in said first elongate structural member **12** configured to couple said ELD **26** to said power source **22** to said CCU for "Lock"/"Unlock" commands and indications.
3. The autonomous security system of claim 1, wherein said barrier control program **34** is configured to enable only one subject **11** at a time to access said UPA during opening/closing of said security barrier apparatus **21**.
4. The autonomous security system of claim 1, wherein said security barrier apparatus **21** further comprises a counterweight configured to balance said opening/closing.
5. The autonomous security system of claim 1, wherein said gear box **20** is configured to rotate said first elongate structural member **12** in a vertical arc to a near vertical position when opened.

WO 2025/041119

PCT/IL2024/050692

6. The autonomous security system of claim 1, wherein said CCU comprises a settings module with adjustable parameters; said adjustable parameters selected from the group consisting of an opening/closing speed adjustment, an opening/closing slowdown feature, and a standard time clock function.
7. The autonomous security system of claim 1, wherein said at least one strip or cable of steel comprises at least two strips or cables of steel.
8. The autonomous security system of claim 7, wherein said at least two strips or cables of steel comprises a plurality of strips or cables of steel.
9. The autonomous security system of claim 1, wherein said first elongate structural member **12** is made from aluminum.
10. The autonomous security system of claim 1, wherein said security barrier apparatus **21** can be fitted with a lower skirt or an upper hi-bar.
11. The autonomous security system of claim 1, wherein said deletion of said stored personal data is automatically initiated after a predetermined interval between storing said personal data and a positive report of no unusual suspicious activity.
12. The autonomous security system of claim 1, wherein said deletion of said stored personal data is automatically initiated after a predetermined interval between storing said personal data and no report on unusual suspicious activity.
13. The autonomous security system of claim 11 or 12, wherein said predetermined interval is about 24 hr.
14. The autonomous security system of any one of claims 1 to 13, further comprising a security sensor **36** interconnected to said user-controlled module **38**, wherein said unusual suspicious activity activates a predetermined signal in said security sensor **36**.
15. The autonomous security system of claim 14, wherein said security sensor **36** is further operably connected to said control center of law enforcement authorities **40**, and said reporting and transferring said stored personal data to said control center **40** is automatically triggered by said predetermined signal from said security sensor **36**.
16. The autonomous security system of any one of claims 1 to 15, wherein said data storage module comprises a personal database of authorized subjects to enter said UPA, further wherein said CCU **30** comprises a program configured to compare between said subject personal data and said personal database, further wherein an unauthorized subject is

WO 2025/041119

PCT/IL2024/050692

determined by the absence of a predetermined match between said subject personal data and said personal database.

17. The autonomous security system of any one of claims 1 to 16, wherein said CCU **30** is interconnected to a phone call center **42** and comprises a phone numbers database of authorized subjects to enter said UPA, further wherein said opening of said security barrier apparatus **21** is after number validation of subject's phone by said phone call center **42**, or after completion of processing and storing said personal data.
18. The autonomous security system of any one of claims 1 to 17, wherein said subject **11** is a driver, and said checkpoint is a vehicle entrance gate.
19. The autonomous security system of claim 18, further comprising an automatic license plate recognition (ALPR) system, configured to capture and record vehicle license plate numbers, and operably connected to said CCU **30**, wherein:
 - a. said vehicle license plate numbers are recognized by said ALPR system, said driver is recognized as an authorized driver and said vehicle entrance gate is opened; and
 - b. said vehicle license plate numbers are not recognized by said ALPR system, said driver is recognized as an unauthorized driver and said vehicle entrance gate is opened after a notification from said data storage module **28** that said personal data was stored.
20. The autonomous security system of any one of claims 1 to 19, wherein said personal data reader interface **19** comprises at least one component selected from the group consisting of:
 - a. a fingerprint scanner;
 - b. an ID card or Driving License scanner;
 - c. a facial camera; and
 - d. a vehicle plate numbers camera.
21. The autonomous security system of any one of claims 1 to 20, further comprising a sign positioned near said kiosk, providing instructions to drivers on a verification process.

WO 2025/041119

PCT/IL2024/050692

22. The autonomous security system of any one of claim 1, wherein said security barrier apparatus **21** is configured for allowing exit of said subject from said UPA.
23. A method for allowing access of an unauthorized subject **11** to an unmanned protected area (UPA) via a checkpoint, comprising steps of:
- a. placing said autonomous security system of any one of claims 1 to 22, adjacent to said checkpoint of said UPA;
 - b. instructing an authorized subject to be identified for entering said UPA **104**;
 - c. instructing said unauthorized subject to provide personal data by said automatic security system **106**; once said personal data storage is completed, said checkpoint gate is opened;
 - d. sending an "Unlock" command to said electromechanical locking device (ELD) by said central control unit (CCU) **108**;
 - e. sending an "Open" indication to said CCU by said ELD **110**;
 - f. sending an "Open" command to said electromechanical motor by said CCU **112**;
 - g. sending an "Open" indication from said electromechanical motor to said CCU **114**;
 - h. sending a "Car-passing" indication to said CCU by an electro-optical sensor (EOS) **116**;
 - i. sending a "Clear" indication to said CCU by said EOS **118**;
 - j. sending a "Close" command to said electromechanical motor by said CCU **120**;
 - k. sending a "Close" indication from said electromechanical motor to said CCU **122**;
 - l. sending a "Lock" command to said ELD by said CCU **124**;
 - m. sending a "Lock" indication to said CCU by said ELD **126**; and
 - n. automatically recording time from said personal data storage **128**:
 - i. if a security breach is reported, then a user-controlled module can be accessed and viewed by a user, said stored personal data can be reported and transferred by said user to a control center of law enforcement authorities, via a secured connection, by providing a user command, for identification of an unauthorized subject suspicious in an unusual activity in said UPA **130**; and

WO 2025/041119

PCT/IL2024/050692

- ii. if there is no unusual activity in said UPA during a predetermined interval from said personal data storage, then said stored personal data is automatically deleted **132**.
24. The method of claim 23, wherein said step (c) of providing said personal data by said unauthorized subject comprises further steps of:
- a. selecting a personal data reader program selected from the group consisting of fingerprint scanning, facial recording, ID card scanning and driving license scanning;
 - b. for said fingerprint scanning, placing a hand on a designated scanning area; for said facial recording, positioning a face within a marked area or aligning it with a camera; for said ID card scanning or driving license scanning, placing an ID card or driving license on said designated scanning area; and
 - c. receiving a notification that said personal data is valid and recorded.
25. The method of claim 23 or 24, comprising placing said autonomous security system of claim 15 in said step (a), and said reporting and transferring said stored personal data to a control center of law enforcement authorities is automatically triggered by said predetermined signal from said security sensor.
26. The method of any one of claims 23 to 25, comprising placing said autonomous security system of claim 16 or 17 in said step (a), further wherein said method comprising after said step (a) and before said step (b), a step of distinguishing between said authorized subject and said unauthorized subject.
27. The method of claim 26, further comprising placing said autonomous security system of claim 16 in said step (a), wherein said step of distinguishing comprises instructing said subject to provide said personal data, further wherein a positive notification indicates that said subject is authorized to access said UPA based on said personal database of said authorized subjects.
28. The method of claim 26, further comprising placing said autonomous security system of claim 17 in said step (a), wherein said step of distinguishing comprises instructing said subject to provide their phone number, further wherein a positive notification indicates that said subject is authorized to access said UPA based on said phone numbers database of said authorized subjects.
29. The method of any one of claims 23 to 28, configured to allow access of an unauthorized driver to said UPA via a vehicle entrance gate, said method comprising placing said

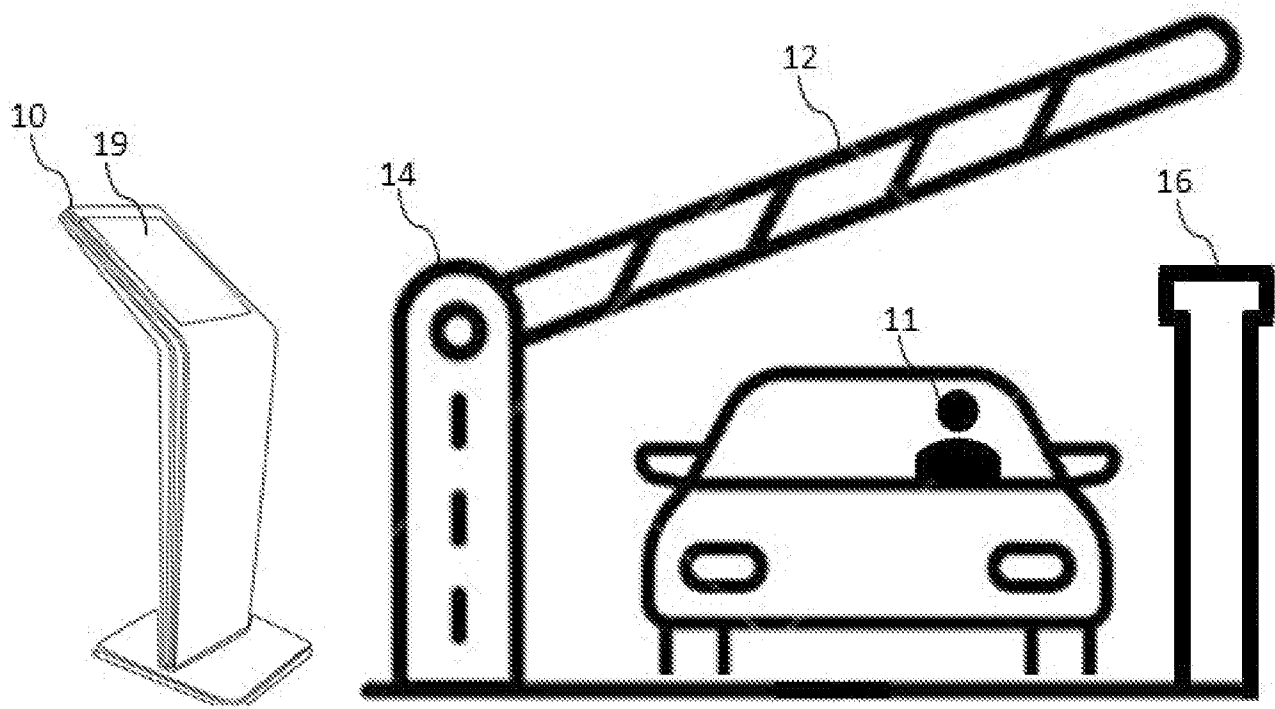
WO 2025/041119

PCT/IL2024/050692

automatic security system of claim 16 in step (a), and said instructing said authorized subject to be identified for entering said UPA in step (b) is by an automatic license plate recognition (ALPR) system.

30. The method of claim 29, wherein dimensions, cameras, and sensors of a kiosk are adjustable to a driver within a vehicle, allowing collecting said personal data without the need of stepping out of said vehicle.

1/7

*Fig. 1*

2/7

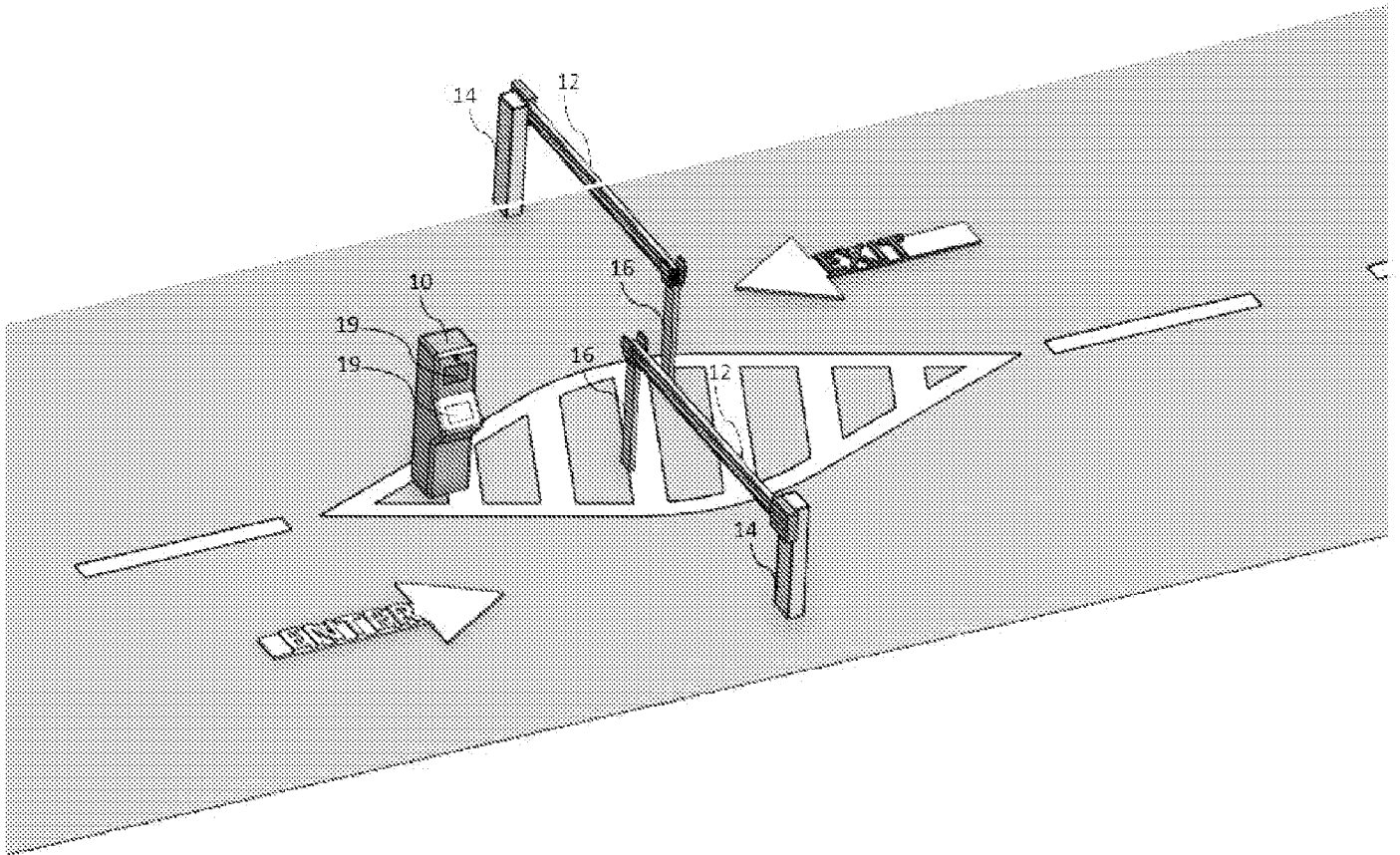


Fig. 2

3/7

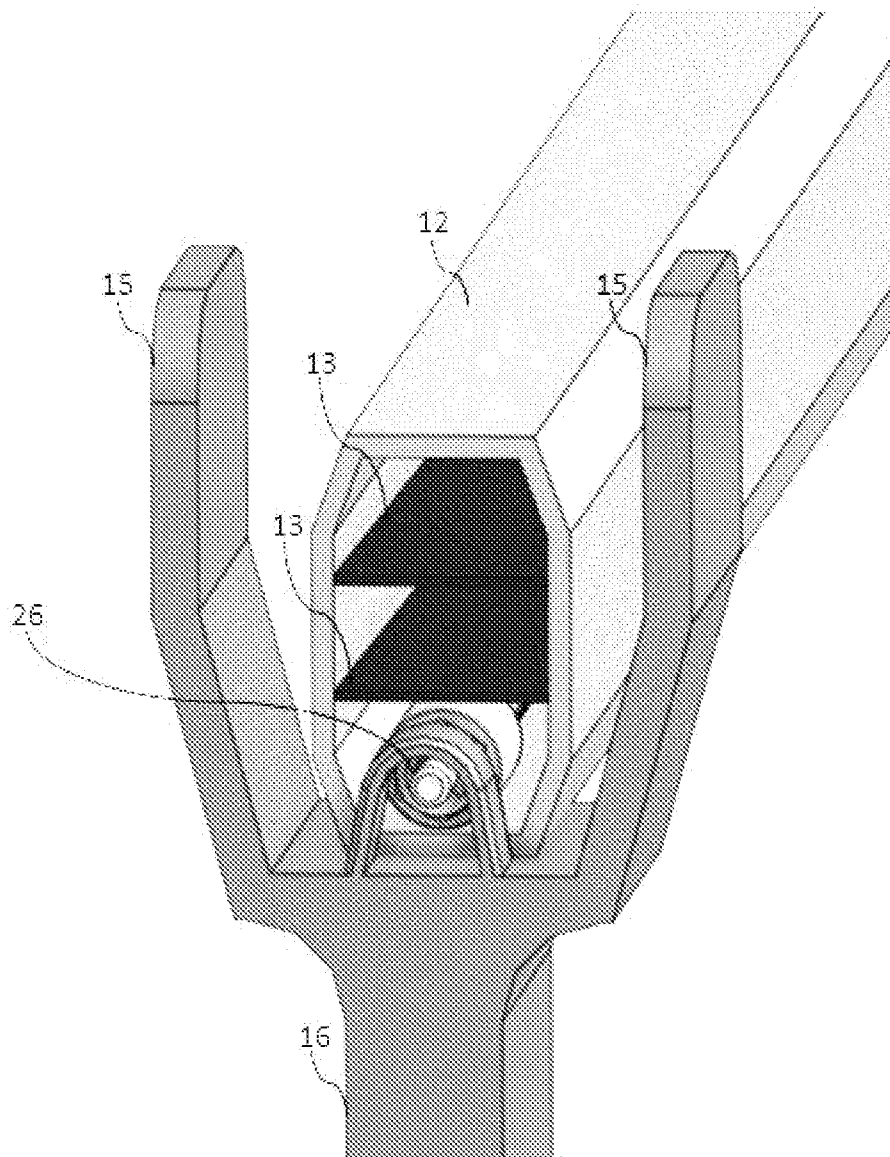


Fig. 3

4/7

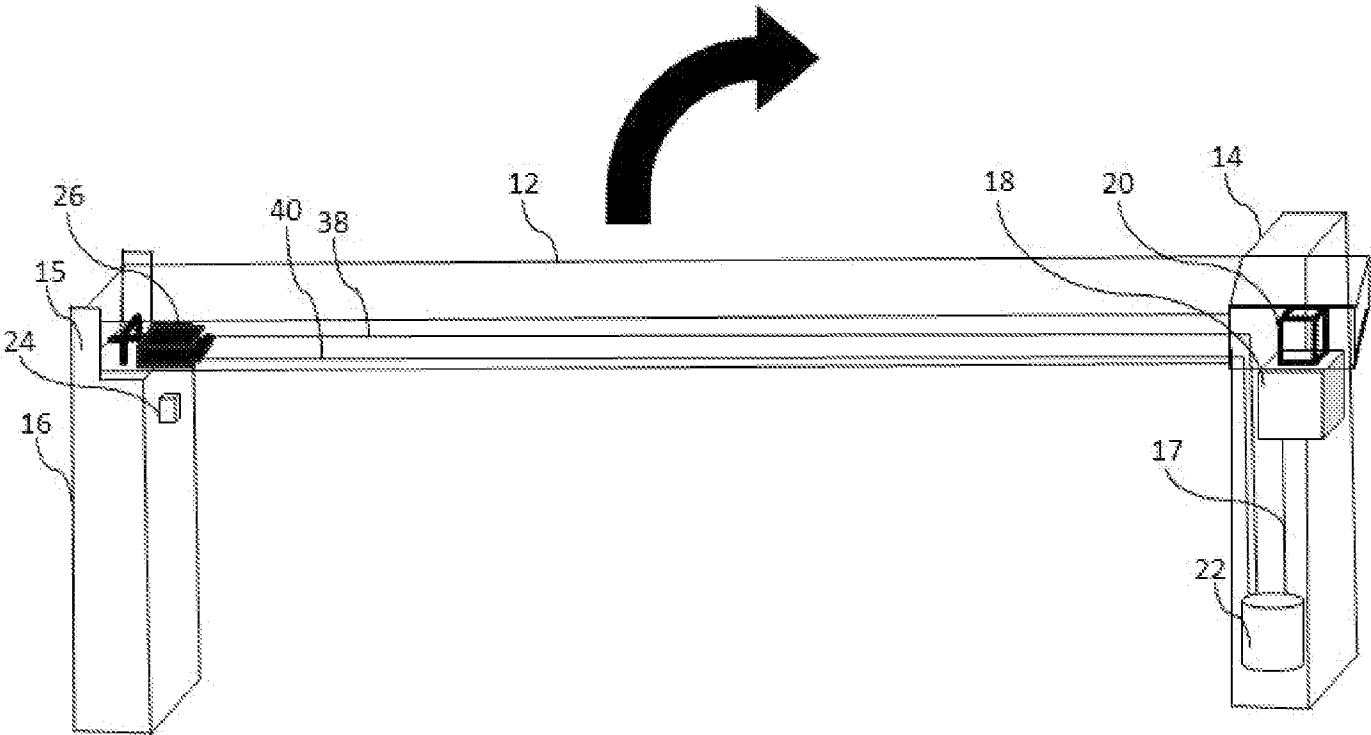


Fig. 4

5/7

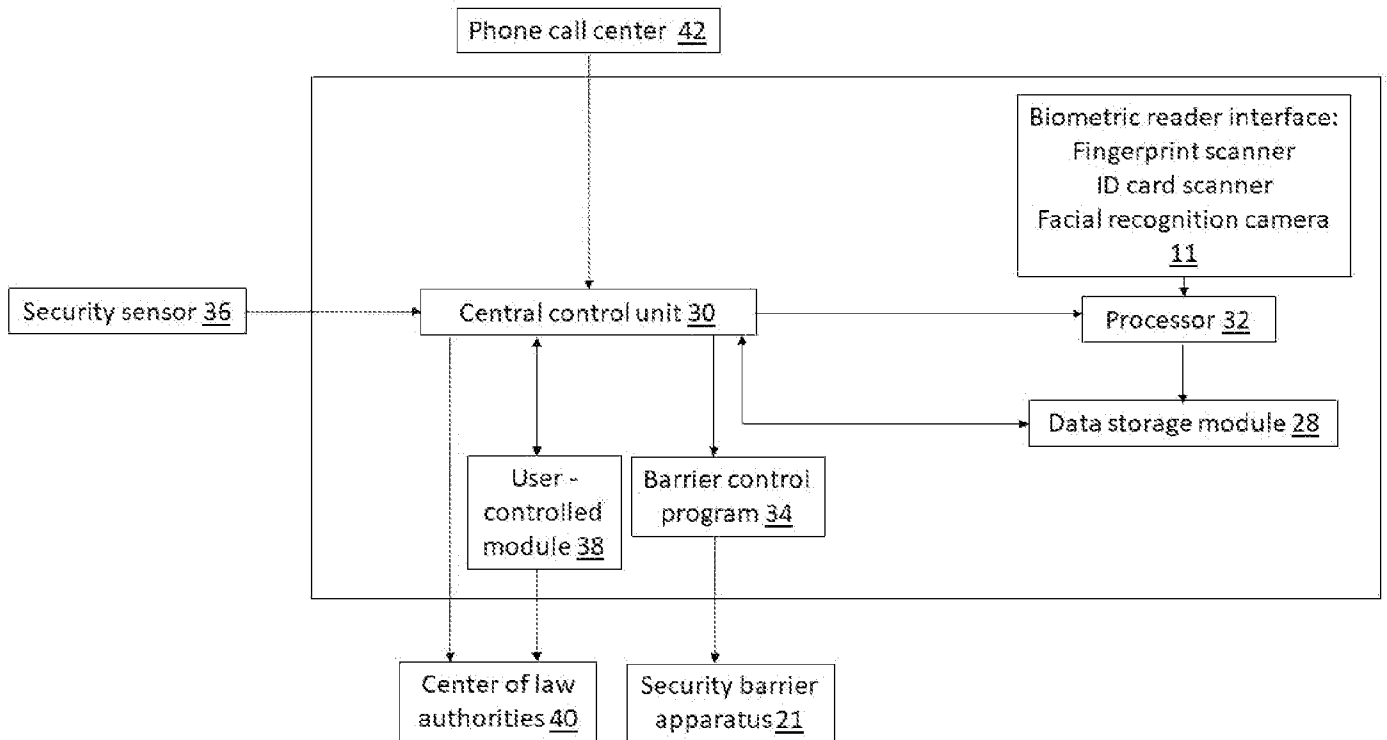


Fig. 5

6/7

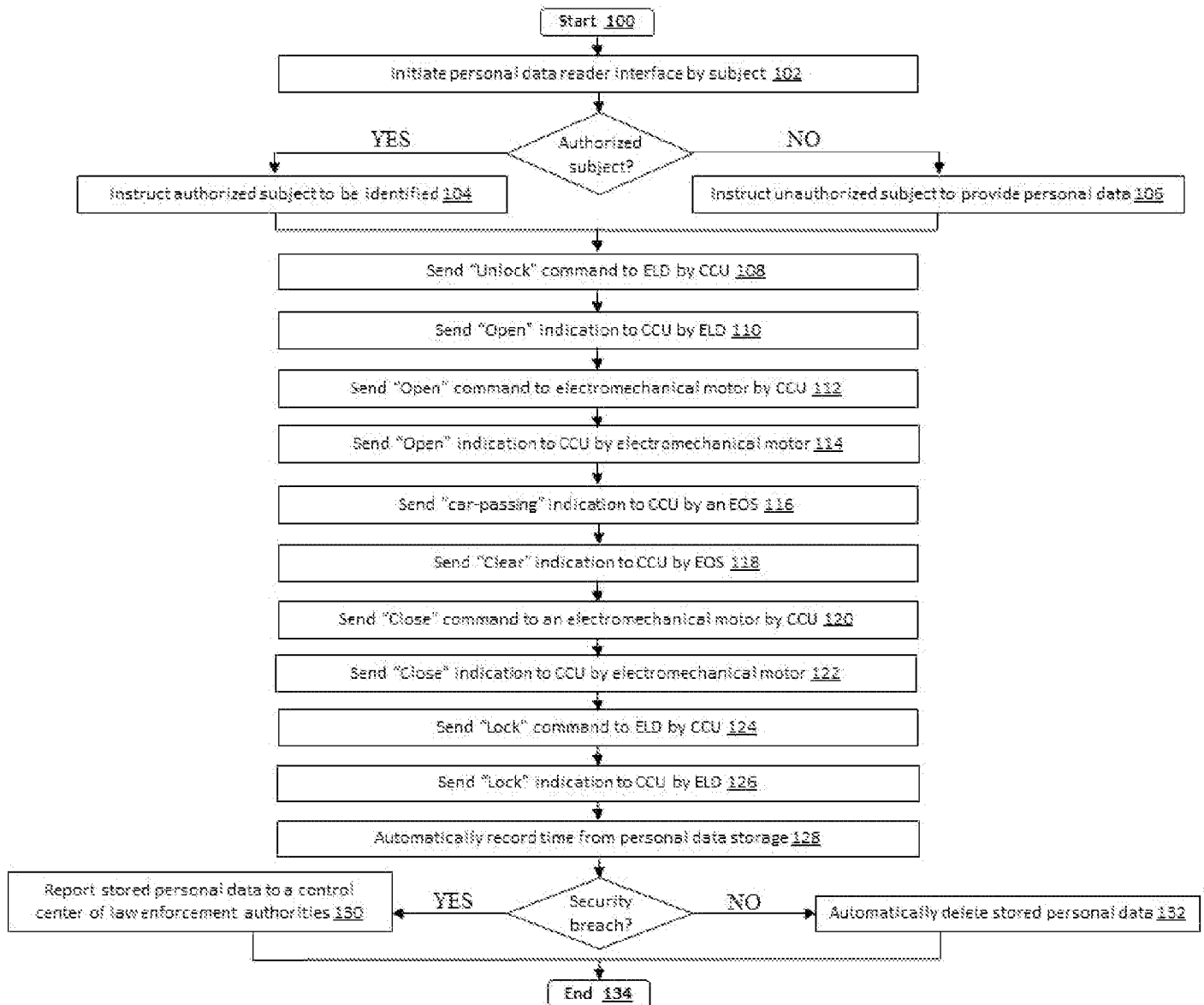


Fig. 6

7/7

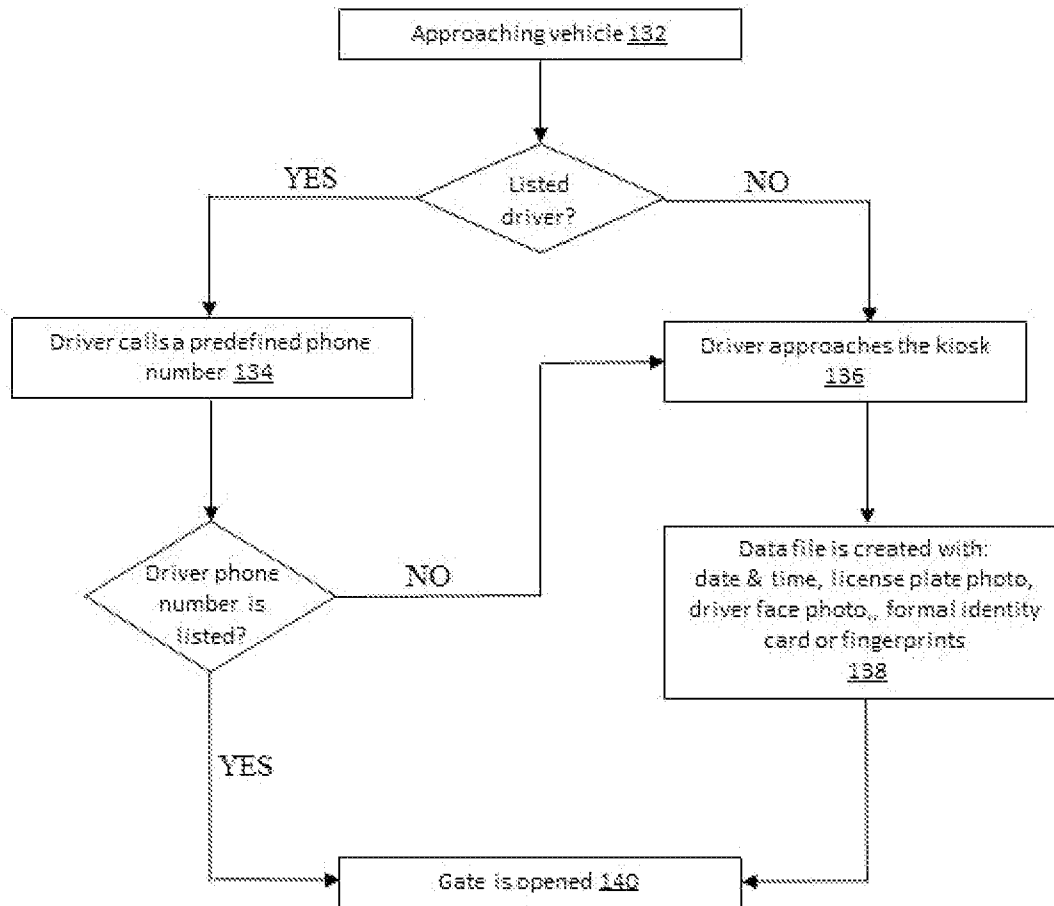


Fig. 7

INTERNATIONAL SEARCH REPORT

International application No.

PCT/IL2024/050692

A. CLASSIFICATION OF SUBJECT MATTER**E01F 13/06**(2024.01)i; **E01F 13/08**(2024.01)i

CPC:E01F 13/06; E01F 13/08

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

E01F 13/06; E01F 13/08

CPC:E01F 13/06; E01F 13/08

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

Databases consulted: Google Patents, Orbit

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	CN 214401538 U (Nanjing Xiecheng Building System Eng Co LTD) 15 October 2021 (2021-10-15) Entire Document	1-30
Y	US 10002476 B1 (Ekin Teknoloji Sanayi ve Ticaret AS) 19 June 2018 (2018-06-19) Entire Document	1-30



Further documents are listed in the continuation of Box C.



See patent family annex.

* Special categories of cited documents:

“A” document defining the general state of the art which is not considered to be of particular relevance

“D” document cited by the applicant in the international application

“E” earlier application or patent but published on or after the international filing date

“L” document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

“O” document referring to an oral disclosure, use, exhibition or other means

“P” document published prior to the international filing date but later than the priority date claimed

“T” later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

“X” document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

“Y” document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

“&” document member of the same patent family

Date of the actual completion of the international search

15 October 2024

Date of mailing of the international search report

15 October 2024

Name and mailing address of the ISA/IL

Israel Patent Office
Technology Park, Bldg.5, Malcha, Jerusalem, 9695101,
Israel
Israel

Telephone No. 972-73-3927202

Email: pctoffice@justice.gov.il

Authorized officer

AMEAR JILANI Yasmin

Telephone No.

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/IL2024/050692

Patent document cited in search report			Publication date (day/month/year)	Patent family member(s)			Publication date (day/month/year)
CN	214401538	U	15 October 2021	CN	214401538	U	15 October 2021
US	10002476	B1	19 June 2018	US	10002476	B1	19 June 2018
				EP	3367344	A1	29 August 2018
				TR	201703006	A2	21 September 2018