

(12) **Österreichische Patentanmeldung**

(21) Anmeldenummer: A 71/2022  
(22) Anmeldetag: 18.03.2022  
(43) Veröffentlicht am: 15.10.2022  
(51) Int. Cl.: **G07C 9/00** (2006.01)

(30) **Priorität:**  
19.03.2021 CH 00295/21 beansprucht.

(71) **Patentanmelder:**  
e-liberty services SA  
2001 Neuchatel 1 (CH)

(74) **Vertreter:**  
Patentanwalt Mikovsky KG  
2100 Korneuburg (AT)

(54) **Verfahren und System zur Kontrolle von Besuchern in einem Zugangsbereich innerhalb eines Freizeitparks**

(57) Verfahren zur Kontrolle von Besuchern (V) in einem Zugangsbereich (7) innerhalb eines Freizeitparks, zum Beispiel eines Skigebiets oder eines Erlebnisparks, das enthält: Senden (100) von Bluetooth-Signalen in Richtung des Zugangsbereichs mit mehreren auf ein gemeinsames Portal (3) montierten Beacons (30), wobei die relative Position der Beacons bekannt ist ;

Filmen (105) des Zugangsbereichs mit Hilfe einer ersten Kamera (31), um ein Standbild oder ein bewegtes Bild (8) des Zugangsbereichs von oben gesehen zu erzeugen; Individualisieren (122) mindestens eines Besuchers in dem Bild;

Empfangen (126) der Position eines Mobilgeräts, zum Beispiel eines Smartphones oder einer Smartwatch, in einem Server (5), die von diesem Mobilgerät mit Hilfe der Bluetooth-Signale bestimmt wird;

Überprüfen (130), ob eine von einem Mobilgerät empfangene Position der Position des individualisierten Besuchers entspricht;

Überprüfen (132) der Zugangsberechtigung des individualisierten Besuchers.

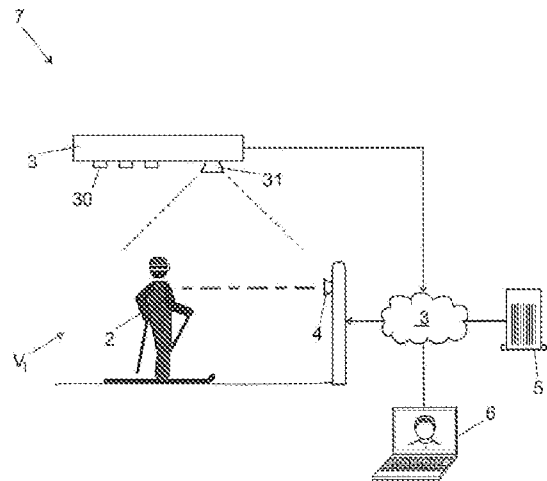


Fig. 1

### Zusammenfassung

Verfahren zur Kontrolle von Besuchern (V) in einem Zugangsbereich (7) innerhalb eines Freizeitparks, zum Beispiel eines Skigebiets oder eines Erlebnisparks, das enthält:

Senden (100) von Bluetooth-Signalen in Richtung des Zugangsbereichs mit mehreren auf ein gemeinsames Portal (3) montierten Beacons (30), wobei die relative Position der Beacons bekannt ist;

Filmen (105) des Zugangsbereichs mit Hilfe einer ersten Kamera (31), um ein Standbild oder ein bewegtes Bild (8) des Zugangsbereichs von oben gesehen zu erzeugen;

Individualisieren (122) mindestens eines Besuchers in dem Bild;

Empfangen (126) der Position eines Mobilgeräts, zum Beispiel eines Smartphones oder einer Smartwatch, in einem Server (5), die von diesem Mobilgerät mit Hilfe der Bluetooth-Signale bestimmt wird;

Überprüfen (130), ob eine von einem Mobilgerät empfangene Position der Position des individualisierten Besuchers entspricht;

Überprüfen (132) der Zugangsberechtigung des individualisierten Besuchers.

Fig. 1

### Technisches Gebiet

Die vorliegende Erfindung betrifft das Problem der Kontrolle von Besuchern in Freizeitparks, insbesondere in Wintersportorten oder Erlebnisparks.

### Stand der Technik

Viele Wintersportorte und Erlebnisparks verwenden RFID-Elemente, zum Beispiel in eine Chipkarte oder eine Uhr integrierte Transponder für die Zugangskontrolle und die Bezahlung der Zugänge. Die Benutzer, die Ski fahren möchten, müssen ein RFID-Element kaufen und es mit einem Geldbetrag laden, um Zugang zu den Anlagen zu erhalten. Die Zahlung erfolgt meist vorab, indem die Karte mit einem vorausbezahlten Betrag geladen wird, der zeitabhängig (zum Beispiel pro Stunde oder Tag) abgebucht wird, oder indem jeder Zugang zu den Anlagen mittels eines RFID-Lesegeräts nahe jedem Zugangsportal kontrolliert wird.

Diese Systeme arbeiten zuverlässig und wirtschaftlich. Die üblichen RFID-Lesegeräte haben aber eine stark reduzierte Reichweite, typischerweise in der Größenordnung von einigen Zentimetern oder einigen Metern. Sie erlauben also nur die Erfassung von Benutzern in direkter Nähe der Zugangskontrollsäulen, aber nicht, sie zu lokalisieren, wenn sie sich von den Anlagen entfernt befinden. Sie erfordern außerdem eine komplexe Logistik für die Verteilung und den Widerruf der RFID-Elemente.

EP3477602A1 beschreibt ein Verfahren und eine Vorrichtung zur Zugangskontrolle und Zahlung in einem Freizeitpark, die eine dedizierte Vorrichtung verwenden. Diese Lösung erlaubt eine präzise Lokalisierung der Benutzer im ganzen Park, macht aber die Verwaltung der Identifikationsvorrichtungen der Benutzer noch komplexer und teurer.

US2017/270734 beschreibt ein System zur Kontrolle von Warteschlangen für Erlebnisparks, das mindestens eine tragbare Vorrichtung und ein Kontrollsystem enthält. Die tragbare Vorrichtung ist mit einer Kennung versehen, die nicht nur einen Zugang zu einer gegebenen Attraktion durch eine NFC-Übermittlung

dieser Kennung an eine NFC-Station, sondern auch eine Erfassung ihrer Position in einer virtuellen Warteschlange, um zu einer der Attraktionen des Parks zu gelangen, erlaubt. Diese Position wird anschließend an die verschiedenen Einheiten des Systems mittels einer Übermittlung mit mittlerer und/oder großer Reichweite übermittelt.

GB2469026 beschreibt ein System, das zum Beispiel in einem Flughafen verwendet werden kann, um die Position eines Passagiers mit Hilfe von Nahfeld-Kommunikationen (RFID-Label), Telekommunikationen (DECT), Kleinzelle, WLAN usw. zu verfolgen, die spezielle Informationen über die Bewegungen des Passagiers liefern und diesen vom Einchecken bis zum Abflug des Flugzeugs oder vom Flugzeug bei seiner Ankunft leiten. Das System kann auch in einem Krankenhaus, einer Multiaktivitäts-Ausstellung, Konferenzen oder Konzerten verwendet werden und Informationen an eine wartende Person liefern.

US2015/091726 betrifft ein System für ein Angebot standortabhängiger Dienste, insbesondere in einem Erlebnispark.

US2014257889 beschreibt ein Lokalisierungssystem von mobilen Geräten, das es ermöglicht, die Wartezeiten in den Warteschlangen abhängig vom Kundenstrom zu optimieren. Es verwendet drahtlose Erfassungsvorrichtungen mobiler Geräte, zum Beispiel mit einer Bluetooth- oder WLAN-Schnittstelle ausgestattete Telefone.

Es sind auch Zahlungs- und Zugangskontrollsysteme zu den Anlagen eines Freizeitparks bekannt, die die Smartphones von Besuchern sowohl zum Zahlen als auch zur Zugangskontrolle der Besucher nutzen. Diese Vorrichtungen nutzen häufig eine drahtlose Schnittstelle in sehr geringer Entfernung, zum Beispiel eine NFC-Schnittstelle (Near Field Communication). Der Besucher muss also sein Smartphone aus seiner Tasche nehmen und es gegen ein NFC-Lesegerät nahe dem Zugangskontrollportal drücken, um die Öffnung dieses Portals zu erlauben. Es ist also notwendig, das Smartphone aus der Tasche zu nehmen, es sogar zu bedienen, was sich zum

Beispiel in einem Wintersportort oder mit Handschuhen als wenig praktisch erweisen kann.

#### Kürze Zusammenfassung der Erfindung

Es ist ein Ziel der vorliegenden Erfindung, ein Verfahren zur Kontrolle von Besuchern in einem Zugangsbereich vorzuschlagen, das nicht die Einschränkungen der obigen Verfahren aufweist.

Ein weiteres Ziel der Erfindung ist ein Verfahren zur Kontrolle von Besuchern in einem Zugangsbereich, das persönliche Vorrichtungen der Besucher verwendet, zum Beispiel Mobilgeräte, aber keine Bedienung im Zugangsbereich erfordert.

Erfindungsgemäß werden diese Ziele insbesondere mittels eines Verfahrens zur Kontrolle von Besuchern in einem Zugangsbereich innerhalb eines Freizeitparks erreicht, zum Beispiel eines Skigebiets oder eines Erlebnisparks, das enthält:

Senden von Bluetooth-Signalen in Richtung des Zugangsbereichs mit mehreren auf ein gemeinsames Portal montierten Beacons, wobei die relative Position der Beacons bekannt ist;

Filmen des Zugangsbereichs mit Hilfe einer nach unten gerichteten ersten Kamera, um ein Standbild oder ein bewegtes Bild des Zugangsbereichs von oben gesehen zu erzeugen;

Individualisieren mindestens eines Besuchers in dem Bild;

Empfangen der Position eines Mobilgeräts, zum Beispiel eines Smartphones oder einer Smartwatch, die mit Hilfe der Bluetooth-Signale bestimmt wird;

Überprüfen, ob eine von einem Mobilgerät empfangene Position der Position des individualisierten Besuchers entspricht;

Überprüfen der Zugangsberechtigung des individualisierten Besuchers.

Das Verfahren ermöglicht so, die Zugangsberechtigungen eines oder mehrerer im Bild eines Zugangsbereichs sichtbaren Besucher zu überprüfen. Es ist dann möglich, diese Information zum Beispiel zu verwenden, um die Besucher ohne Zugangsberechtigung

zu erfassen, und/oder um den über eine solche Zugangsberechtigung verfügenden Besuchern den Zugang zu erlauben.

Dieses Verfahren erfordert nicht, dass die Besucher dedizierte Geräte verwenden, sondern nur ein Mobilgerät wie ein Smartphone oder eine Smartwatch, mit dem die meisten sowieso ausgerüstet sind.

Eine spezielle Softwareanwendung ("App") kann in das Mobilgerät geladen werden, um seine Position auf der Basis der von den verschiedenen Beacons empfangenen Bluetooth-Signale zu bestimmen.

Das Verfahren kann einen Schritt der Bestimmung mindestens eines nicht berechtigten Besuchers, dessen mit dem Bild bestimmte Position nicht einer empfangenen Position entspricht, oder mindestens eines nicht berechtigten Besuchers enthalten, der keine Zugangsberechtigungen zum kontrollierten Zugangsbereich besitzt.

Ein Besucher wird als nicht berechtigt angesehen, wenn er sich in dem Zugangsbereich befindet, aber zum Beispiel:

Kein Mobilgerät hat oder sein Mobilgerät ausgeschaltet ist;  
die dedizierte Softwareanwendung nicht installiert oder gestartet hat;

die erforderlichen Bluetooth-Dienste in seines Mobilgeräts nicht gestartet hat;

nicht beweisen kann, dass er gültige Zugangsberechtigungen zum kontrollierten Bereich besitzt.

So ist es möglich, automatisch die Anwesenheit eines solchen nicht berechtigten Besuchers im Zugangsbereich zu bestimmen und dementsprechend zu handeln.

Die Reaktion auf die Anwesenheit eines nicht berechtigten Besuchers kann die Erfassung eines Bilds dieses nicht berechtigten Besuchers mit Hilfe einer zusätzlichen Kamera enthalten. Dieses Bild kann auf dem Endgerät einer Aufsichtsperson angezeigt werden, die zum Beispiel den nicht berechtigten

Besucher abfangen und ihm den Zugang zum kontrollierten Bereich verbieten oder ihm einen Zugang verkaufen kann.

Das Verfahren kann die Markierung eines Bildabschnitts enthalten, der den nicht berechtigten Besucher enthält. Dies ermöglicht es der Aufsichtsperson, ohne weiteres zu bestimmen, welcher Besucher in einer Gruppe von Besuchern oder in einer Warteschlange nicht berechtigt ist.

Die Position des Mobilgeräts kann von jedes Mobilgeräts bestimmt und an einen Server gesendet werden. Dies ermöglicht es, die Rechenleistung zu verteilen und gleichzeitig eine große Anzahl von gleichzeitig nahe dem Portal anwesenden Benutzern zu lokalisieren.

Jedes Mobilgeräts kann seine Position mithilfe der Bluetooth-Methode AOD (Angle of Departure) unter Verwendung von von den Beacons gesendeten Bluetooth-Signalen bestimmen.

Die Beacons können aus Sendeantennen eines Bluetooth-Low-Energy-Signals bestehen.

Die Beacons können in mehreren Gruppen oder Ankern auf dem Portal verteilt sein. Die Beacons sind mindestens einer Antenne der gleichen Gruppe näher als der nächstliegenden Antenne einer anderen Gruppe.

Jede Gruppe von Beacons kann mehrere Beacons aufweisen, die matrixförmig angeordnet sind. Jede Matrix kann mindestens  $N=1$  Zeilen und  $M>1$  Spalten aufweisen. Die verschiedenen Beacons einer Gruppe können auf eine gleiche leitende Platte montiert sein, zum Beispiel eine PCB-Karte.

Alle Beacons innerhalb jeder Gruppe können mit einem gemeinsamen Bluetooth-Sender verbunden sein.

Alle Beacons können mit einem gemeinsamen Bluetooth-Sender verbunden sein.

Die Beacons innerhalb jeder Gruppe können abwechselnd senden.

Die Beacons können nacheinander auf mehreren verschiedenen Bluetooth-Kanälen senden. Dies ermöglicht es, den Einfluss des

zum Beispiel durch Reflexionen der Bluetooth-Signale verursachten Rauschens zu minimieren.

Die Beacons werden vorzugsweise auf ein gleiches Substrat montiert, zum Beispiel eine gleiche Leiterplatte. Dies ermöglicht es, eine präzise relative Positionierung der Beacons im Werk zu garantieren.

Das Substrat kann anschließend auf das Portal montiert werden.

Das Portal kann über dem Zugangsbereich platziert werden, damit die Besucher unter dem Portal durchgehen müssen, um zum kontrollierten Bereich zu gelangen.

Die von den Beacons gesendeten Bluetooth-Signale werden vorzugsweise von einem gleichen Sender erzeugt.

Die erste Kamera ist vorzugsweise eine Kamera mit Entfernungsmessung. Dies ermöglicht es, die verschiedenen Besucher auf einem Bild bequemer zu individualisieren, indem die verschiedenen Ebenen differenziert werden. Dies ermöglicht es auch, die Position jedes Besuchers zweidimensional zu bestimmen und eine Information über seine Größe zu haben.

Die erste Kamera ist vorteilhafterweise auf das Portal montiert. Dies ermöglicht es, eine präzise und stabile relative Positionierung zwischen den Beacons und der ersten Kamera zu garantieren. Diese Positionierung erleichtert die Entsprechung zwischen den Positionen der individualisierten Besucher auf dem Bild und den von den Mobilgeräten bestimmten Positionen.

Die Erfindung hat auch ein System zur Kontrolle von Besuchern in einem Zugangsbereich innerhalb eines Freizeitparks, zum Beispiel eines Skigebiets oder eines Erlebnisparks, zum Gegenstand, das enthält:

ein Portal;

auf das Portal montierte Beacons;

einen Sender, der so mit den Beacons verbunden ist, dass diese Beacons Bluetooth-Signale in Richtung des Zugangsbereichs senden;

eine nach unten gerichtete erste Kamera, um den Zugangsbereich zu filmen, um ein Standbild oder ein bewegtes Bild des Zugangsbereichs von oben gesehen zu erzeugen;

ein Softwaremodul, um mindestens einen Besucher in dem Bild zu individualisieren;

ein Softwaremodul, um die Position eines Mobilgeräts, zum Beispiel eines Smartphones oder einer Smartwatch, die durch dieses Mobilgeräts bestimmt wird, zu empfangen;

ein Softwaremodul, um zu überprüfen, ob eine von einem Mobilgerät empfangene Position der Position eines individualisierten Besuchers entspricht;

ein Softwaremodul, um die Zugangsberechtigung des individualisierten Besuchers zu überprüfen.

Das System kann eine zusätzliche Kamera enthalten, um ein Frontbild der nicht berechtigten Besucher im Zugangsbereich zu erfassen.

#### Kurze Beschreibung der Figuren

Anwendungsbeispiele der Erfindung sind in der Beschreibung angegeben, die durch die beiliegenden Figuren veranschaulicht wird, in denen:

- Figur 1 eine schematische Ansicht eines Systembeispiels zur Durchführung der Erfindung veranschaulicht.

- Figur 2 ein Bild eines Zugangsbereichs von oben gesehen veranschaulicht.

- Figur 3 ein Bild eines Zugangsbereichs von vorne gesehen veranschaulicht.

- Figur 4 ein Beispiel eines Flussdiagramms eines Verfahrens gemäß der Erfindung veranschaulicht.

#### Ausführungsbeispiel(e) der Erfindung

Ein Beispiel eines Systems gemäß der vorliegenden Erfindung ist schematisch in Figur 1 veranschaulicht. Es ist dazu bestimmt, die Zugangsberechtigungen von Besuchern  $V_i$  in einen Freizeitpark zu kontrollieren, zum Beispiel ein Skigebiet oder ein Erlebnispark. Das System kann verwendet werden, um den Hauptzugang zum

Freizeitpark zu kontrollieren, zum Beispiel, um nur die Besucher einzulassen, die eine gültige Eintrittskarte erworben haben, oder um die Zugänge zu Attraktionen oder zu Skiliften zu kontrollieren, wenn die Besucher sich innerhalb dieses Freizeitparks befinden, zum Beispiel um diese Zugänge zu fakturieren, die Anzahl von Besuchern zu zählen, die Besucherströme zu verwalten, usw.

In diesem Beispiel ist das System über ein Skigebiet als Beispiel von Freizeitparks ausgebreitet, um den Zugang von Besuchern, zum Beispiel Skifahrern, zu einem Skilift dieser Station zu kontrollieren. Andere Freizeitparks, einschließlich Erlebnisparks, Ferienclubs, Open-Air-Festivals usw. können das System verwenden.

Der Freizeitpark weist mehrere Anlagen auf, hier Skilifte. Der Zugang von Besuchern  $V_i$  zu jeder Anlage wird von einem Portal 3 über dem Zugangsbereich 7 und/oder einer Säule neben diesem Zugangsbereich kontrolliert. Die Zugangskontrolle kann die Öffnungskontrolle einer Schleuse, zum Beispiel eines Drehkreuzes oder einer Tür, beinhalten, die Zugang zur Anlage verschafft. In einer bevorzugten Ausführungsform ist der Zugang zumindest zu manchen Anlagen möglich, ohne durch eine Schleuse zu gehen. Die Zugangskontrolle zielt dann darauf ab, zu kontrollieren, welcher Besucher zu welchem Zeitpunkt zu welcher Anlage gelangt ist, und/oder eine Anzeige zu übertragen, wenn ein Besucher ohne Zugangsberechtigungen sich in der Nähe des kontrollierten Zugangsbereichs befindet. In diesem Fall kann die Zugangskontrollsäule zum Beispiel verwendet werden, um die nicht berechtigten Besucher zu erfassen und zu identifizieren, die sich zum Beispiel in einer Warteschlange befinden.

Die Besucher  $V_i$  müssen mit eines Mobilgeräts 2 ausgestattet sein, zum Beispiel einem Smartphone, einer Smartwatch, usw., um ihre Zugangsberechtigung zu beweisen. Zusätzliche Zugangskontrolleinrichtungen, zum Beispiel ein RFID-Kartenleser, können vorgesehen werden, um die Besucher zu kontrollieren, die keine

solche Mobilgeräte haben, oder wenn die Batterie ihres Mobilgeräts entladen ist. Eine Softwareanwendung ("App"), die der Zugangskontrolle dediziert ist, muss im Mobilgerät 2 installiert sein und zum Zeitpunkt der Zugangskontrolle ausgeführt werden.

Das Portal 3 ist mit mehreren Beacons 30 ausgestattet, die Bluetooth-Signale senden. Optional kann mindestens ein Teil der Beacons auf eine Säule in Höhe der Teilnehmer montiert sein. Die Position der verschiedenen Beacons ist bekannt. In einer Ausführungsform haben die Beacons einen Abstand zueinander von weniger als oder gleich  $\lambda/2$ , zum Beispiel einen Abstand gleich  $\lambda/3$ , wobei  $\lambda$  die Wellenlänge des Bluetooth-Signals ist (etwa 12,5 cm bei 2,4 GHz). Diese Anordnung ermöglicht eine hohe Auflösung der Präzisionsmessung mit einer gegebenen Anzahl von Beacons. Die erwünschte hohe Auflösung wird auch dank einer sorgfältigen Anordnung der Beacons erhalten, zum Beispiel einer Anordnung in einer Linie, einer Matrix oder einem Kreis, und dank einer ausreichenden Anzahl von Beacons.

Die Beacons 30 werden vorteilhafterweise auf eine am Portal befestigte einzige Leiterplatte montiert, was es ermöglicht, die präzise Positionierung der Beacons im Werk zu garantieren. Es ist auch möglich, mehrere Leiterplatten mit mehreren Beacons 30 auf jeder Platte vorzusehen. Jede Leiterplatte, Anker genannt, trägt eine Gruppe von Beacons 30.

Das von den verschiedenen Beacons 30 gesendete Signal wird von einem einzigen gemeinsamen elektronischen Sender erzeugt, zum Beispiel eine Funkanlage Bluetooth Low Energy 5.1 oder einer höheren Version. Die Verwendung eines einzigen Senders ermöglicht es, eine Phasenverschiebung zu garantieren, die nur von der Position der verschiedenen Beacons abhängt. Der Sender kann mit den verschiedenen Beacons durch alternierend offene analoge Schalter verbunden sein, damit die verschiedenen Beacons abwechselnd senden. Um die Positionierung zu einem Zeitpunkt "t" durchzuführen, kann eine einzige Bluetooth-Nachricht verwendet werden, die in verschiedene Teile (ebenso viele wie es Beacons

gibt) geteilt werden kann, die je von einem Beacon gesendet werden.

Die Position jedes Mobilgeräts 2 kann von diesem Mobilgerät bestimmt und an den Server 5 gesendet werden. Dies ermöglicht es, die für diese Lokalisierung notwendige Rechenleistung zu verteilen und so gleichzeitig eine große Anzahl von gleichzeitig nahe dem Portal anwesenden Benutzern zu lokalisieren.

Zu diesem Zweck wird der Abstrahlwinkel der von den verschiedenen Beacons 30 gesendeten Bluetooth-Signale vorteilhafterweise durch jedes Mobilgerät 2 bestimmt, die sie empfängt, und von diesem Mobilgerät verwendet, um seine Position durch Triangulation zu bestimmen.

Es ist auch möglich, den Auftreffwinkel der von den Mobilgeräten empfangenen Signale zu verwenden, um seine Position zu bestimmen. Es ist auch möglich, die Position der Mobilgeräten 2 im Server oder in der Cloud zu berechnen.

Die Beacons können in mehrere Gruppen (Anker genannt) auf dem gleichen Portal 3 verteilt sein. Jeder Beacon ist mindestens einer Antenne der gleichen Gruppe näher als der nächstliegenden Antenne einer anderen Gruppe. Der Abstand zwischen zwei benachbarten Beacons der gleichen Gruppe ist vorzugsweise geringer als 20 Zentimeter, zum Beispiel geringer als 10 Zentimeter. Der Abstand zwischen zwei Gruppen ist vorzugsweise größer als 30 Zentimeter. Die verschiedenen Gruppen können in einer Richtung lotrecht zur Durchquerungsrichtung des Portals zueinander beabstandet sein.

Jede Gruppe kann eine Matrix von Beacons aufweisen, wobei jede Matrix mindestens  $N=1$  Zeilen und  $M>1$  Spalten aufweist.

Alle Beacons 30 innerhalb jeder Gruppe können auf eine gleiche Platte montiert sein, zum Beispiel eine gleiche PCB-Karte.

Alle Beacons 30 innerhalb jeder Gruppe können mit einem gemeinsamen Bluetooth-Sender verbunden sein. Die Beacons können über einen Demultiplexer verbunden sein, der das Bluetooth-Signal

abwechselnd an die verschiedenen Beacons der Gruppe sendet. Innerhalb jeder Gruppe senden die Beacons also zyklisch abwechselnd.

Alle Beacons der verschiedenen Gruppen können über einen Demultiplexer mit einem gemeinsamen Bluetooth-Sender verbunden sein.

Die Beacons können nacheinander auf mehreren verschiedenen Bluetooth-Kanälen senden. Dies ermöglicht es, den Einfluss des zum Beispiel durch Reflexionen der Bluetooth-Signale verursachten Rauschens zu minimieren.

Es ist zum Beispiel möglich, jedes Mal von einem Bluetooth-Kanal zu einem anderen Bluetooth-Kanal umzuschalten, wenn das Bluetooth-Signal von einem Beacon 30 zu einem anderen umgeschaltet wird.

Es ist möglich vorzusehen, dass ein Beacon nacheinander auf mehreren verschiedenen Kanälen sendet, um den Einfluss des Rauschens zu minimieren.

Mindestens eine Kamera 31 filmt den Zugangsbereich. Die relative Position der Kamera 31 ist bezüglich der Beacons 30 ortsfest. Die Kamera 31 kann auf das Portal 3 montiert werden und den Zugangsbereich 7 von oben fixieren. Die Kamera 31 kann auf die gleiche Leiterplatte montiert werden wie die Beacons 30, oder in einer bezüglich der Leiterplatte ortsfesten Position montiert werden.

Die Kamera 31 kann eine RGB-Kamera sein, um im sichtbaren Bereich zu filmen. Sie kann auch eine Infrarot-Kamera sein, um ein Bild zu filmen, das weniger von den Schatten oder Spiegelungen abhängt. In einer vorteilhaften Ausführungsform ist die Kamera 31 eine Entfernungsmesskamera (depth-of-field), die die Entfernung zu den gefilmten Objekten und Personen im Zugangsbereich 7 misst. Es ist auch möglich, mehrere Kameras zu verwenden, zum Beispiel zwei stereoskopische Kameras, um den Zugangsbereich 7 aus verschiedenen Richtungen zu filmen.

Eine mit einer oder mehreren Frontkameras 4 versehene Säule kann vorgesehen werden, um die Besucher  $V_i$  im Zugangsbereich in Frontansicht (von vorne) zu filmen.

Die Kamera 31 und die optionale Kamera 4 senden Bilder oder Bildfolgen an einen Server 5. Der Server kann auf das Portal 3 montiert oder in Abstand eingebaut und über ein Netz zugänglich sein, zum Beispiel Internet, ein zellulARES Netz, WLAN, usw. Der Server 5 kann auch in der Cloud sein oder mehrere miteinander verbundene Maschinen aufweisen.

Ein auf dem Server 5 ausgeführtes Softwaremodul ermöglicht es, die von der Kamera 31 aufgenommene Folge von Bildern von oben zu analysieren. Ein Beispiel eines solchen Bilds ist in Figur 2 veranschaulicht; man sieht mehrere Besucher  $V_1, V_1, V_n$ , hier Skifahrer, sowie Geräte des Zugangsbereichs 7, zum Beispiel Schranken 70, um die Besucher zu lenken. Das Softwaremodul führt eine Bildvorverarbeitung durch, um es neu zu rahmen, den Kontrast, die Helligkeit, die Schärfe usw. zu korrigieren. In einem zweiten Schritt ermöglicht das Softwaremodul, die verschiedenen Besucher zu individualisieren, d.h. zu bestimmen, welche Abschnitte des Bilds 2D oder 2,5D einem Besucher entsprechen. Die Individualisierung kann auf einer Bildanalyse basieren. Ein System künstlicher Intelligenz ermöglicht es, die Vordergrundabschnitte (die durch die Entfernungsmessung und/oder durch Kontrasterfassung bestimmt werden können, zum Beispiel, wenn der Boden weiß ist) einzuordnen und zu bestimmen, welche zu einem Besucher gehören. Die Bildanalyse ermöglicht es vorteilhafterweise, zwischen zwei nebeneinander stehenden Besuchern zu unterscheiden, da die Form der Einheit nicht derjenigen eines einzelnen Besuchers entspricht. Die Unterscheidung zwischen Besuchern kann auch auf der Entfernungsmessung basieren, zum Beispiel, indem die Maxima lokaler Höhen bestimmt werden, die den Scheiteln des Schädels oder des Helms jedes Besuchers entsprechen. In dem Fall, in dem der Zugangsbereich von mehreren Kameras 31 gefilmt wird, zum Beispiel stereoskopischen Kameras,

kann die Analyse auch eine 3D-Wiederherstellung der Szene im Zugangsbereich enthalten, um die verschiedenen Besucher noch besser zu individualisieren.

Das Softwaremodul führt vorzugsweise eine Verfolgung ("Tracking") der individualisierten Besucher auf mehreren aufeinanderfolgenden Bildern aus, um die für jedes Bild notwendige Rechenleistung zu reduzieren und die Zuverlässigkeit der Individualisierung zu verbessern. Diese Verfolgung ermöglicht es, den Weg des Schwerpunkts und des Volumens jedes Besuchers zu erhalten.

Das Softwaremodul bestimmt auch den Schwerpunkt  $CG_i$  in 2D oder 3D jedes Besuchers  $V_i$ .

Das Mobilgerät 2 der Besucher empfängt über seine Bluetooth-Schnittstelle die von den verschiedenen Beacons 30 gesendeten phasenverschobenen Signale und bestimmt seine relative Position zu mehreren aufeinanderfolgenden Zeitpunkten. Diese Position wird anschließend in einer Nachricht an den Server 5 übertragen, zum Beispiel einer Folge von Nachrichten oder einem Datenstrom.

In einer alternativen Ausführungsform empfängt das Mobilgerät 2 der Besucher über seine Bluetooth-Schnittstelle von den verschiedenen Beacons 30 gesendete phasenverschobene Signale, misst diese Phasenverschiebung und überträgt diese Phasenverschiebungen an den Server 5, der die relative Position des Mobilgeräts 2 bestimmt.

Das Softwaremodul empfängt diese Nachricht oder diese Nachrichten und überprüft, ob eine Nachricht von einem Mobilgerät 2 empfangen wird, die eine Position anzeigt, die der Position  $CG_i$  eines der individualisierten Besucher entspricht.

Im Fall einer Übereinstimmung überprüft der Server 5 anschließend, ob der Besucher  $V_i$  eine gültige Zugangsberechtigung besitzt. Hierzu kann er vom Besucher eine Nachricht anfordern, vorzugsweise elektronisch signiert, die seine Zugangsberechtigungen anzeigt. Diese Nachricht kann auch in der Nachricht enthalten sein, die die Position des Besuchers anzeigt. Die

Zugangsüberprüfung kann auch einen "Challenge-Response"-Mechanismus beinhalten, während dessen der Server 5 eine Frage (die Challenge) an das Mobilgerät 2 des individualisierten Besuchers stellt, auf die dieses Mobilgeräts nur korrekt antworten kann, wenn sie Zugangsberechtigungen besitzt.

Wenn kein Mobilgerät eine einem individualisierten Besucher entsprechende Position überträgt, oder wenn ein der Position eines Besuchers entsprechendes Mobilgerät 2 nicht beweisen kann, dass es Zugangsberechtigungen besitzt, ist dieser im Bild 8 anwesende Besucher nicht berechtigt. Er kann als solcher auf dem Bild 8 markiert werden, wenn dieses Bild auf dem Endgerät einer Aufsichtsperson angezeigt wird. Es ist auch möglich, diese Information zu verwenden, um die Öffnung einer Zugangskontrollschleuse zu blockieren, wenn eine solche Schleuse vorgesehen ist.

In einer bevorzugten Ausführungsform nimmt die Frontkamera ein statisches oder bewegtes Bild 9 des Zugangsbereichs 7 auf, wie man in Figur 3 sieht, und markiert in diesem Bild den nicht berechtigten Besucher  $V_i$  mit einer Markierung 301. Die Markierung kann zum Beispiel die Bildbereichsumgebung enthalten, die den nicht berechtigten Besucher enthält, die Leuchtstiftmarkierung dieses Bereichs, usw. Das so markierte Bild 9 wird auf dem Endgerät 6 einer Aufsichtsperson angezeigt, die so den nicht berechtigten Besucher abfangen und von ihm zum Beispiel einen anderen Fahrausweis verlangen kann. Es ist auch möglich, auf dem Endgerät der Aufsichtsperson das von der ersten Kamera 31 aufgenommene Bild 8 anzuzeigen und optional zu markieren.

Ein Beispiel eines erfindungsgemäßen Verfahrens wird nun ausführlicher in Verbindung mit Figur 4 beschrieben. Die erste Spalte dieser Figur ist ein Flussdiagramm der von den Beacons 30 ausgeführten Vorgänge. Die zweite Spalte ist ein Flussdiagramm der von der Draufsicht-Kamera 31 und der zugeordneten Sendelelektronik ausgeführten Vorgänge. Die dritte Spalte ist ein Flussdiagramm der von jedem Mobilgerät 2 ausgeführten Vorgänge,

deren Anwendung aktiviert ist. Die vierte Spalte ist ein Flussdiagramm der vom Server 5 ausgeführten Vorgänge.

Während des Schritts 100 senden die Beacons 30 auf dem Portal 3 Bluetooth-Signale in Richtung des Zugangsbereichs 7. Die Beacons 30 haben keine anderen Aktionen auszuführen und müssen daher nicht mit dem Server 5 verbunden sein; sie können es aber sein, um sie zu aktivieren oder zu deaktivieren.

Während des Schritts 105 erfasst die Kamera 31 ein Standbild oder ein bewegtes Bild 8 des Zugangsbereichs 7 von oben gesehen. Dieses Bild wird anschließend während des Schritts 106 an den Server 5 gesendet, zum Beispiel über eine Funkschnittstelle, WLAN oder anderes. Die Folge wird wiederholt, um einen Videostrom oder eine Folge von Standbildern zu erzeugen.

In einer anderen Ausführungsform ist ein Computer direkt mit den Kameras 31 und 4 verbunden. Dieser Computer steuert die Kameras, führt die Verarbeitung der Bilder durch und sendet die Zugangsanforderungen und die Durchgangsinformationen der Besucher an den Server 5.

Während des Schritts 110 empfängt das Mobilgerät 2 jedes Besuchers im Zugangsbereich, der Bluetooth aktiviert hat, die von den Beacons 30 gesendeten Bluetooth-Signale.

Während des Schritts 112 bestimmt ein von mindestens bestimmten dieser Mobilgeräten 2 ausgeführte Softwareanwendung die Position dieses Mobilgeräts ausgehend von den Phasenunterschieden zwischen den von den verschiedenen Beacons empfangenen Signalen, was es ihm erlaubt, den Abstrahlwinkel dieser Signale und von daher die relative Position des Mobilgeräts 2 bezüglich der Beacons 30 zu bestimmen. Diese relative Position wird während des Schritts 114 an den Server 5 gesendet, zum Beispiel in Form einer Nachricht, indem in den Server 5 geschrieben wird, usw.

Während des Schritts 116 übermittelt die Anwendung mindestens bestimmter Mobilgeräten ihre Zugangsberechtigungen zum kontrollierten Bereich an den Server 5. Dieser Schritt kann spontan oder auf Anforderung ausgeführt werden, zum Beispiel kann

das Mobilgerät eine Antwort auf eine vom Server 5 empfangene Challenge senden, um ihre Zugangsberechtigungen zu beweisen.

Die Übermittlungen von den Mobilgeräten 2 zum Server 5 sind vorzugsweise elektronisch signiert, um es dem Server 5 zu erlauben, sich zu vergewissern, dass die empfangenen Positionen und Zugangsberechtigungen sehr wohl von der vorgesehenen Mobilgeräten 2 kommen, und ein anderes Mobilgerät daran zu hindern, eine Identität unrechtmäßig zu verwenden.

Während des Schritts 120 empfängt das Softwaremodul im Server 5 ein Bild 8 oder einen Videostrom von der Kamera 31. Während des Schritts 122 führt dieses Softwaremodul eine Vorverarbeitung des empfangenen Bilds 8 aus und individualisiert dann die verschiedenen im Bild dargestellten Besucher  $V_i$ . Diese Individualisierung kann durch Bildverarbeitung und/oder auf der Basis der Tiefeninformationen ausgeführt werden, die vom Entfernungsmesssensor der Kamera 31 geliefert werden.

Während des Schritts 124 bestimmt das Softwaremodul die einzelne Position jedes individualisierten Besuchers im Bild 8, zum Beispiel die Position ihres Massezentrums  $CG_i$ . Die Position kann mit Hilfe der Kamera mit Entfernungsmessung 31 in 2D oder vorzugsweise in 3D bestimmt werden.

Während des Schritts 126 empfängt der Server 5 die Position jedes Geräts, das sie ihm übermittelt hat. Dieser Empfang kann jederzeit und wiederholt stattfinden.

Während des Schritts 128 überprüft das Softwaremodul des Servers 5 die Zugangsberechtigungen jedes Geräts, das sie übermittelt hat. Diese Überprüfung kann nach dem Empfang einer Nachricht von diesem Mobilgerät oder auf Anforderung des Servers erfolgen. In einer Ausführungsform enthält die Überprüfung eine Identifizierung oder eine Authentifizierung des Mobilgeräts 2, mit einem Identifizierungs- oder Authentifizierungsprotokoll, dann die Überprüfung der Zugangsberechtigungen des identifizierten oder authentifizierten Besuchers in einer für den Server zugänglichen Datenbank.

Während des Schritts 130 überprüft das Softwaremodul des Servers 5 für jeden während des Schritts 122 individualisierten Besucher, ob die Position dieses Besuchers im Zugangsbereich 7, die während des Schritts 124 ausgehend von den Bildern der Kamera 31 bestimmt wird, der während des Schritts 126 empfangenen Position eines Mobilgeräts 2 entspricht.

Eine Übereinstimmung wird zum Beispiel festgestellt, wenn der Abstand zwischen dem Schwerpunkt  $CG_i$  des Besuchers  $V_i$ , bestimmt ausgehend vom Bild 8, und der während des Schritts 124 empfangenen Position eines Mobilgeräts einen Schwellwert nicht überschreitet, zum Beispiel 50 cm. Der Abstand kann in 3D gemessen werden; es ist tatsächlich unwahrscheinlich, dass ein Besucher sein Mobilgerät zum Beispiel nahe dem Boden oder über seinem Kopf trägt. In einer Variante kann eine Übereinstimmung festgestellt werden, wenn die von dem Mobilgerät 2 übertragene Position einem Abschnitt in 2D oder in 3D des individualisierten Besuchers entspricht.

Wenn kein Mobilgerät 2 eine Position anzeigt, die einem individualisierten Besucher  $V_i$  entspricht, wird das Verfahren im Schritt 134 fortgesetzt. Im gegenteiligen Fall, wenn der individualisierte Besucher  $V_i$  ein Mobilgerät besitzt, das mit der Anwendung ausgestattet ist, die eine Position entsprechend derjenigen des Besuchers im Bild 8 sendet, wird das Verfahren im Schritt 132 fortgesetzt, während dessen eine Entscheidung abhängig von den Zugangsberechtigungen dieses Besuchers getroffen wird.

Wenn die Zugangsberechtigungen gültig sind, und wenn der Besucher berechtigt ist, Zugang zum kontrollierten Bereich zu haben, kehrt das Verfahren zum Schritt 120 zurück. In einer Variante wird der Besucher gezählt. Es ist auch möglich, ein mit diesem Besucher verbundenes Geldkonto zu belasten, um ihm den Zugang zu berechnen. Das Verfahren kann auch die Öffnung einer optionalen Schleuse aufweisen, um den Durchgang des berechtigten Besuchers zu erlauben.

Im gegenteiligen Fall, d.h. wenn der individualisierte Besucher  $V_i$  keine Zugangsberechtigungen zum kontrollierten Bereich besitzt, wird das Verfahren im Schritt 134 fortgesetzt. Während dieses Schritts wird ein Standfoto oder ein bewegtes Foto des Besuchers von der Frontkamera aufgenommen. Der nicht berechtigte Besucher kann auf diesem Bild mittels einer Markierung 301 markiert werden. Das so erfasste Bild wird an das Endgerät einer in der Nähe befindlichen Aufsichtsperson übertragen, um zum Beispiel den Durchgang dieses nicht berechtigten Besuchers zu blockieren, ihm eine Eintrittskarte zu verkaufen oder von ihm zu verlangen, seine Zugangsberechtigung auf andere Weise zu beweisen.

Anstelle vom oder zusätzlich zum Schritt 134 können andere Reaktionen während des Schritts 136 vorgenommen werden, um auf die Anwesenheit eines nicht berechtigten Besuchers im Zugangsbereich 7 zu reagieren. Es ist zum Beispiel möglich, eine optionale Schleuse zu blockieren, eine akustische und/oder visuelle Warnung (zum Beispiel die Anzeige einer Nachricht auf einem vom Empfangsbereich aus sichtbaren Bildschirm) zu senden, oder eine Nachricht auf das Mobilgerät dieses Besuchers zu senden, um es ihm zu ermöglichen, eine Zugangsberechtigung zu kaufen, oder von ihm zu verlangen, den Zugangsbereich 7 zu verlassen.

In den Figuren verwendete Bezugszeichen

- V Besucher
- 2 Mobilgerät
- 3 Portal
- 30 Beacons
- 31 mit dem Portal verbundene Kamera
- 4 Frontkamera
- 5 Server
- 6 Endgerät eines Zugangskontrolleurs
- 7 Zugangsbereich
- 70 Schranken
- 8 Bild des Zugangsbereichs von oben, erfasst mit der mit dem Portal verbundenen Kamera 31
- 9 Frontbild des Zugangsbereichs, erfasst mit der Frontkamera 4
- 100 Senden von Bluetooth-Signalen durch die Beacons 30
- 105 Erfassen eines Draufsichtbilds 8 des Zugangsbereichs 7
- 106 Senden des Draufsichtbilds 8 des Zugangsbereichs an den Server 5
- 110 Empfang der Signale der Beacons 30
- 112 Bestimmen der Position des Mobilgeräts
- 114 Senden einer Nachricht mit der Position des Mobilgeräts und seine Zugangsberechtigungen
- 120 Empfang des Draufsichtbilds des Zugangsbereichs 7 im Server 5
- 122 Bildverarbeitung und Individualisierung von Besuchern  $V_i$  auf dem Draufsichtbild
- 124 Bestimmen der Position der individualisierten Besucher ausgehend von dem Draufsichtbild 8
- 126 Empfang der Nachrichten der Besucher  $V_i$  mit der Position ihres Mobilgeräts
- 128 Überprüfen der Zugangsberechtigungen der Besucher  $V_i$
- 130 Für jeden individualisierten Besucher, Überprüfen, ob

eine empfangene Nachricht eine Position des Mobilgeräts anzeigt, die der Position des Besuchers entspricht, die ausgehend vom Bild 8 bestimmt wird

- 132 Für jeden individualisierten Besucher, Überprüfen der Zugangsberechtigungen des Mobilgeräts 2 zur entsprechenden Position
- 134 Erfassen oder Sichern eines Frontfotos 9 eines individualisierten aber nicht berechtigten Besuchers
- 136 Andere Reaktion auf die Anwesenheit eines individualisierten aber nicht berechtigten Besuchers
- 201 Markierung eines Besuchers auf dem Bild 200
- 301 Markierung eines Besuchers auf dem Bild 300

## Patentansprüche

1. Verfahren zur Kontrolle von Besuchern (V) in einem Zugangsbereich (7) innerhalb eines Freizeitparks, zum Beispiel eines Skigebiets oder eines Erlebnisparks, das enthält:

Senden (100) von Bluetooth-Signalen in Richtung des Zugangsbereichs mit mehreren auf ein gemeinsames Portal (3) montierten Beacons (30), wobei die relative Position der Beacons bekannt ist;

Filmen (105) des Zugangsbereichs mit Hilfe einer nach unten gerichteten ersten Kamera (31), um ein Standbild oder ein bewegtes Bild (8) des Zugangsbereichs von oben gesehen zu erzeugen;

Individualisieren (122) mindestens eines Besuchers in dem Bild;

Erhalten (126) der Position eines Mobilgeräts, zum Beispiel eines Smartphones oder einer Smartwatch, in einem Server (5), die mit Hilfe der Bluetooth-Signale bestimmt wird;

Überprüfen (130), ob eine von einem Mobilgerät empfangene Position der Position des individualisierten Besuchers entspricht;

Überprüfen (132) der Zugangsberechtigung des individualisierten Besuchers.

2. Verfahren nach Anspruch 1, wobei die Position des Mobilgeräts von dem Mobilgerät bestimmt und vom Server empfangen wird.

3. Verfahren nach einem der Ansprüche 1 oder 2, das einen Schritt der Bestimmung mindestens eines nicht berechtigten Besuchers, dessen mit dem Bild (8) bestimmte Position nicht einer empfangenen Position entspricht, oder mindestens eines nicht berechtigten Besuchers enthält, der keine Zugangsberechtigungen zum kontrollierten Zugangsbereich besitzt.

4. Verfahren nach Anspruch 3, das die Erfassung (134) eines Bilds (9) des nicht berechtigten Besuchers mit Hilfe einer zusätzlichen Kamera (4) enthält.

5. Verfahren nach einem der Ansprüche 1 bis 4, das die Markierung (301) eines den nicht berechtigten Besucher enthaltenden Bildabschnitts (9) enthält.

6. Verfahren nach einem der Ansprüche 2 bis 5, wobei das Mobilgerät (2) seine Position mit Hilfe der Bluetooth-Methode AOD (Angle of Departure) bestimmt.

7. Verfahren nach Anspruch 6, wobei Bluetooth-Signale von den mehreren Beacons (30) gesendet werden, die in mehreren Gruppen auf dem Portal verteilt sind, wobei die Antennen jeder Gruppe in Matrixform angeordnet sind.

8. Verfahren nach einem der Ansprüche 6 oder 7, wobei ein Bluetooth-Sender ein Signal nacheinander über einen Demultiplexer an mehrere Beacons sendet.

9. Verfahren nach einem der Ansprüche 6 bis 8, wobei ein Bluetooth-Signal von den Beacons (30) nacheinander in mehrere unterschiedliche Kanäle gesendet wird.

10. Verfahren nach einem der Ansprüche 6 bis 9, wobei ein Bluetooth-Signal nacheinander von mehreren Beacons (30) in mehrere unterschiedliche Kanäle gesendet wird.

11. Verfahren nach einem der Ansprüche 7 bis 10, wobei die Beacons (30) jeder Gruppe auf ein gleiches Substrat auf dem Portal montiert werden, zum Beispiel eine gleiche Leiterplatte.

12. Verfahren nach einem der Ansprüche 1 bis 11, wobei die erste Kamera (31) eine Kamera mit Entfernungsmessung ist.

13. Verfahren nach einem der Ansprüche 1 bis 12, wobei die erste Kamera (31) auf das Portal (3) montiert ist.

14. System zur Kontrolle von Besuchern (V) in einem Zugangsbereich (7) innerhalb eines Freizeitparks, zum Beispiel eines Skigebiets oder eines Erlebnisparks, das enthält:

ein Portal (3)

auf das Portal (3) montierte Beacons (30);

einen mit den Beacons verbundenen Sender, so dass diese Beacons Bluetooth-Signale in Richtung des Zugangsbereichs (7) senden;

eine nach unten gerichtete erste Kamera (31), um den Zugangsbereich (7) zu filmen, um ein Standbild oder ein bewegtes Bild (8) des Zugangsbereichs von oben gesehen zu erzeugen;

ein Softwaremodul, um mindestens einen Besucher in dem Bild (8) zu individualisieren;

ein Softwaremodul, um die durch dieses Mobilgerät bestimmte Position eines Mobilgeräts, zum Beispiel eines Smartphones oder einer Smartwatch, zu empfangen;

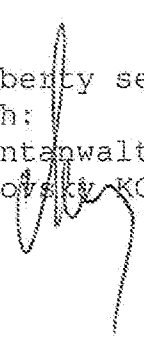
ein Softwaremodul, um zu überprüfen, ob eine empfangene Position eines Mobilgeräts der Position eines individualisierten Besuchers entspricht;

ein Softwaremodul, um die Zugangsberechtigung des individualisierten Besuchers zu überprüfen.

15. System nach Anspruch 14, das eine zusätzliche Kamera (4) enthält, um ein Frontalbild der nicht berechtigten Besucher im Zugangsbereich zu erfassen.

Korneuburg, - 5. MAI 2022

e-liberty services SA  
durch:  
Patentanwalt  
Mikšovičský KG



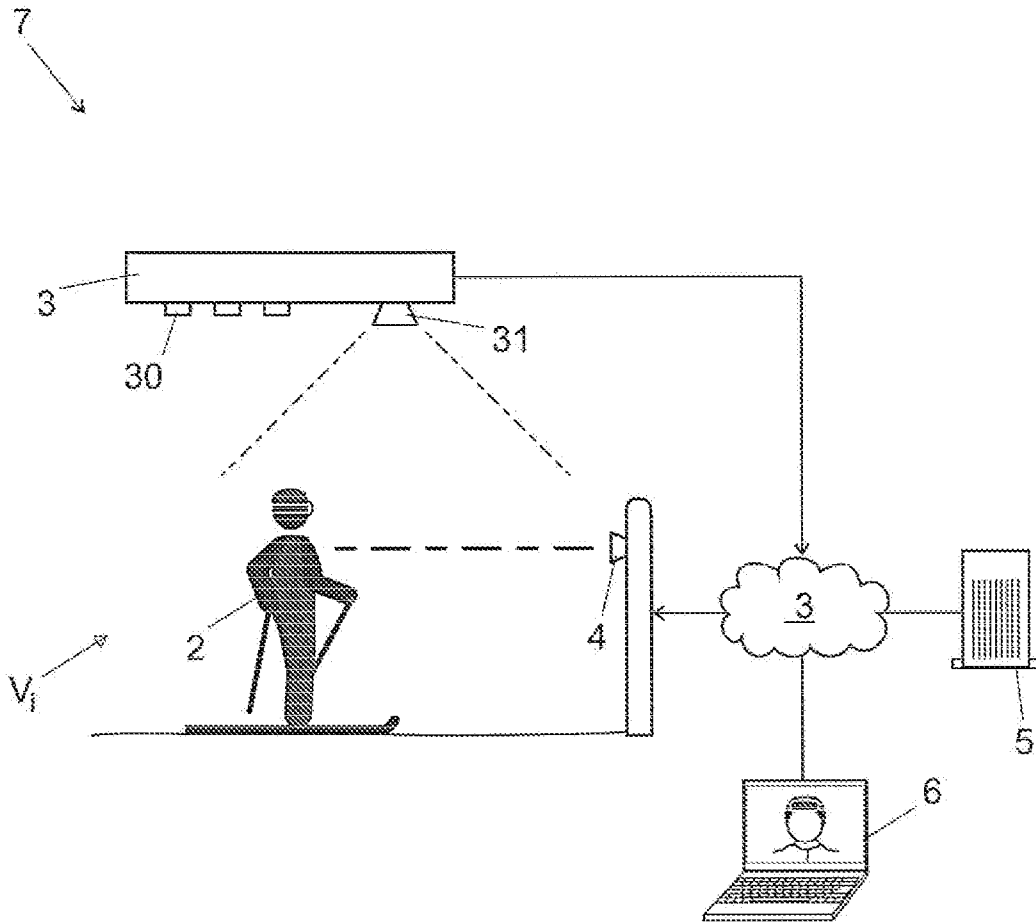


Fig. 1

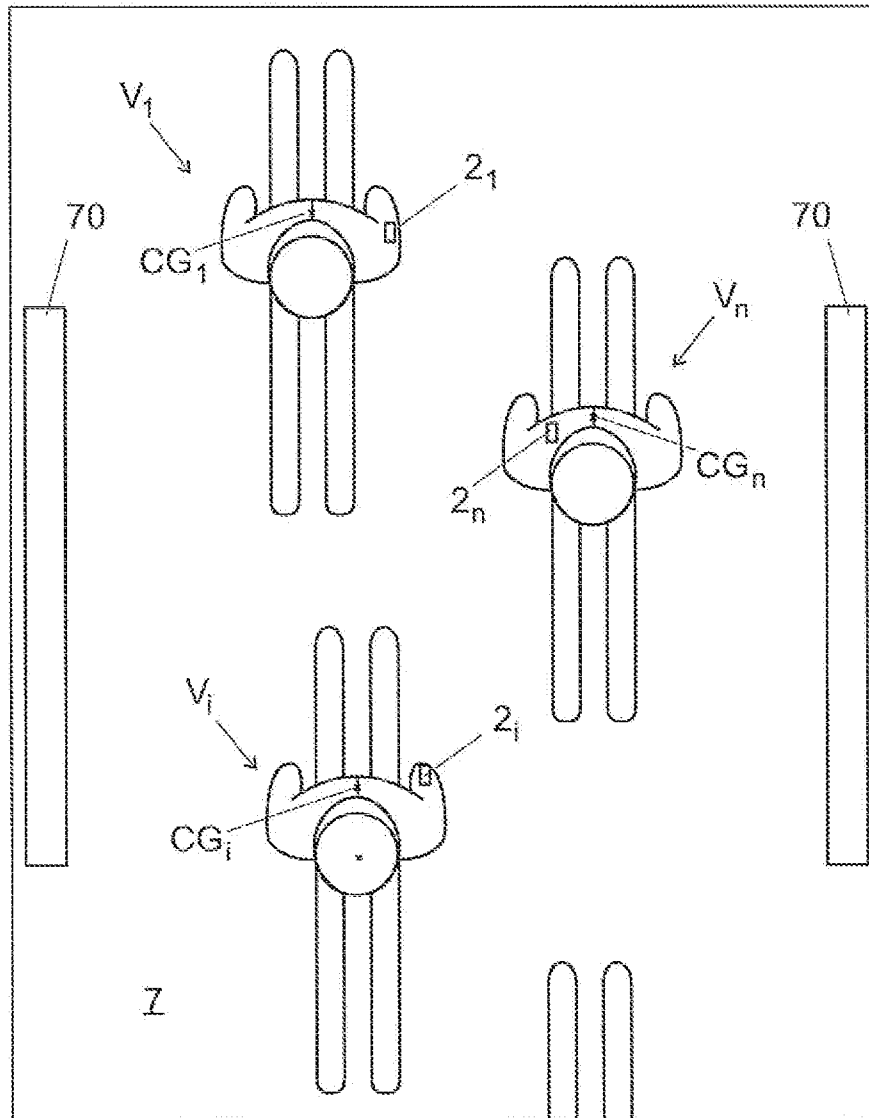


Fig. 2

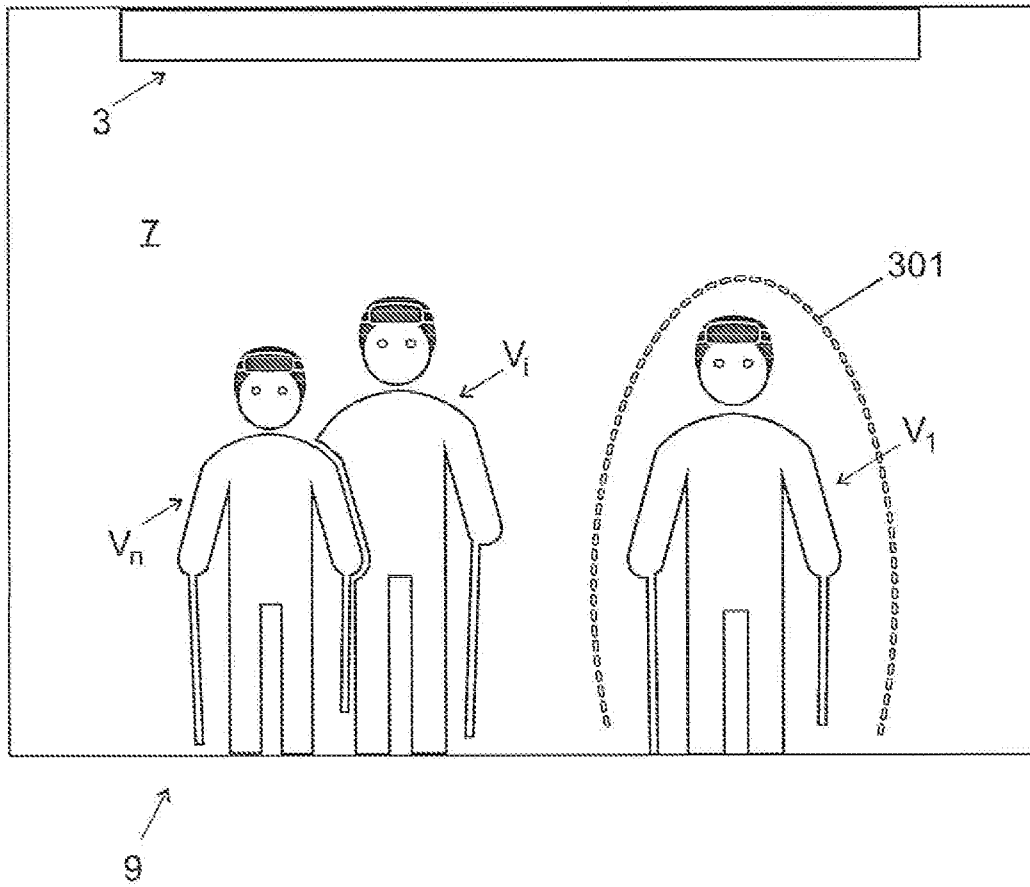


Fig. 3

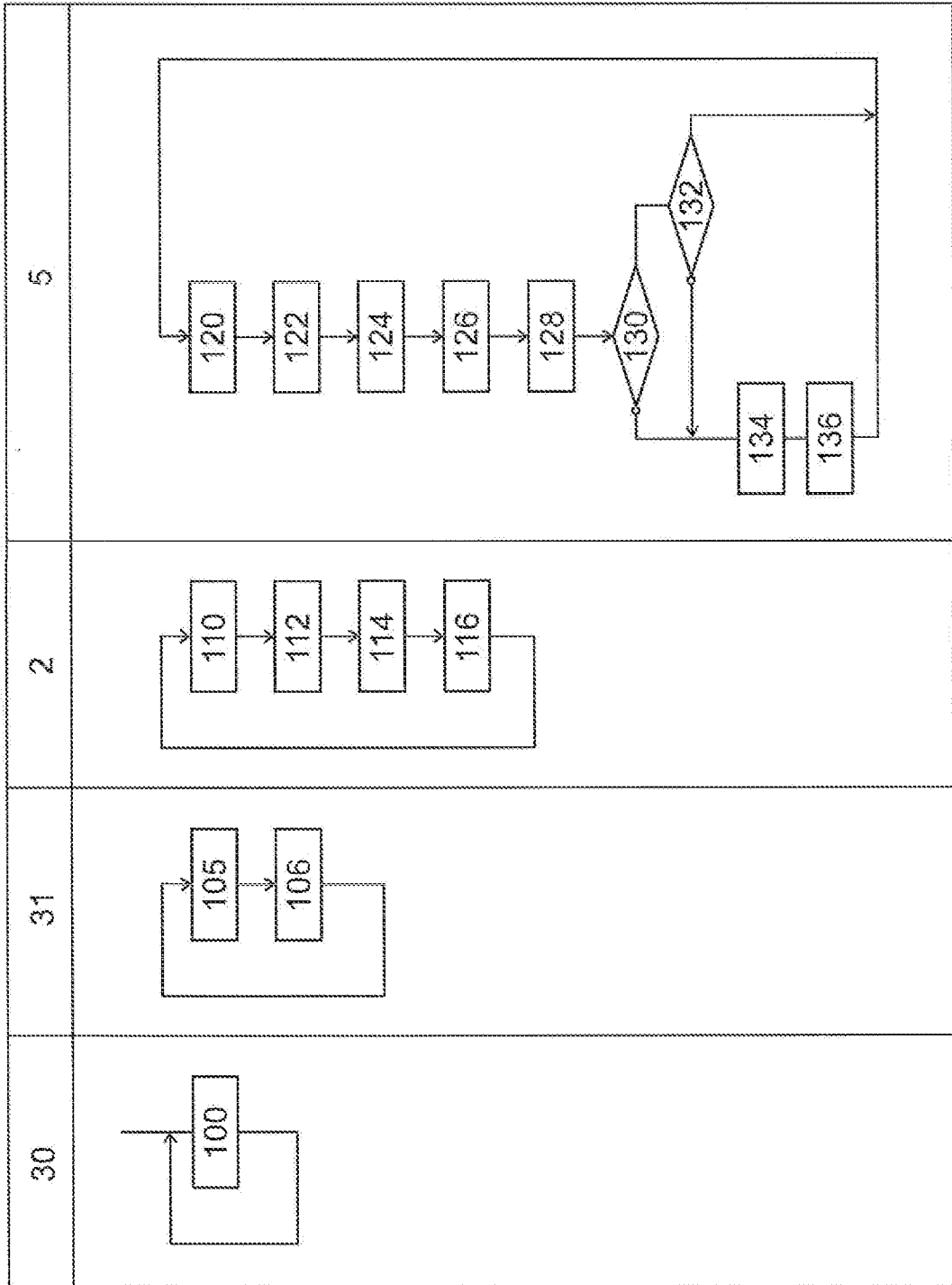


Fig. 4