(19) Евразийское патентное ведомство

(11) 043458 (13) B1

(12) ОПИСАНИЕ ИЗОБРЕТЕНИЯ К ЕВРАЗИЙСКОМУ ПАТЕНТУ

(45) Дата публикации и выдачи патента
2023.05.25

(21) Номер заявки
202192439

(22) Дата подачи заявки
2020.04.29

(51) Int. Cl. ***G07C 9/25*** (2020.01)
G08B 25/00 (2006.01)

(54) СИСТЕМА БЕЗОПАСНОСТИ, СОДЕРЖАЩАЯ УСТРОЙСТВО УПРАВЛЕНИЯ ДОСТУПОМ С ЭЛЕКТРОННОЙ БЛОКИРОВКОЙ, И СПОСОБ РАЗБЛОКИРОВКИ ЭТОГО УСТРОЙСТВА

(31) **62/839,968; 62/893,368; 63/009,381**
(32) **2019.04.29; 2019.08.29; 2020.04.13**
(33) **US**
(43) **2022.03.31**
(86) **PCT/CA2020/050567**
(87) **WO 2020/220127 2020.11.05**

(71)(73) Заявитель и патентовладелец:
ЭКТИВ ВИТНЕСС КОРП. (CA)

(72) Изобретатель:
Бакши Раджив Кумар, Блэк Дэвид Аллан (CA), Вейл Джозеф П. (US)

(74) Представитель:
Нилова М.И. (RU)

(56) CN-A-110032921
WO-A1-2019056988
CN-A-108121977
CN-A-107066942

(57) Предложены различные варианты осуществления автоматической системы безопасности, позволяющей человеку получить доступ в пространство после аутентификации. Также предложены различные варианты осуществления способов разблокировки электронного устройства управления доступом системы безопасности. С применением системы и способа выполняют двухэтапную аутентификацию, в которой по меньшей мере один этап включает оценку черт лица, включающий этап, который включает представление скорректированных черт лица. Указанная система и способы могут использоваться для предотвращения или ограничения доступа людям в пространство, для доступа к которому они не имеют прав.

043458 B1

043458 B1

Родственная заявка

В заявке на данное изобретение испрашивается приоритет по предварительной заявке на патент США № 62/839,968, поданной 29 апреля 2019 г.; предварительной заявке на патент США № 62/893,368, поданной 29 августа 2019 г.; и предварительной заявке на патент США № 63/009,381, поданной 13 апреля 2020 г.; полное содержание патентных заявок 62/839,968; 62/893,368 и 63/009,381 включено в настоящий документ посредством ссылки.

Уровень техники

Настоящее изобретение относится к системам и способам безопасности и, в частности, к системам и способам безопасности, включающим биометрическую аутентификацию.

Область техники

В нижеследующих абзацах представлено описание уровня техники настоящего изобретения. Однако их включение в настоящий документ не означает, что все, что в них обсуждается, является предшествующим уровнем техники или частью информации, известной специалистам в данной области техники.

Многие системы безопасности были созданы для управления доступом к пространствам, содержащим ценности или ресурсы. К таким пространствам относятся физические пространства, такие как жилые и рабочие пространства, и электронные пространства, содержащие ценную информацию, например банкомат. Относительно недавно системы безопасности стали включать в себя автоматизированные системы аутентификации, которые предполагают ограничение прямого взаимодействия между лицом, осуществляющим доступ к защищенному пространству, и лицом, ответственным за управление таким доступом, или не предполагают такого взаимодействия. Использование таких автоматизированных систем аутентификации обычно считается предпочтительным, поскольку они позволяют уменьшить или исключить человеческий фактор или слабые стороны, а также снизить затраты, связанные с работой системы безопасности.

Однако существенная специфическая техническая проблема, связанная с системами автоматической аутентификации, состоит в проектировании и конфигурировании компонентов системы, с помощью которых система аутентификации предоставляет доступ человеку, имеющему право доступа к системе, и, наоборот, отказывает в доступе человеку, который взаимодействует с системой аутентификации, но не имеет прав доступа к системе. Системы аутентификации, работа которых основана на уникальных и неизменных биометрических характеристиках, таких как отпечатки пальцев или черты лица, в этом отношении считаются системами строгой аутентификации. Тем не менее известно, что недобросовестным людям известны способы обхода даже этих биометрических систем аутентификации, например, путем представления изображения лица или видео на камеру системы аутентификации. Таким образом, люди, незаконно получившие доступ, могут обмануть владельцев ценностей.

Еще одна проблема, связанная с известными автоматизированными системами распознавания лиц, заключается в том, что, если хранилища данных содержат данные о чертах лица большого количества людей, правильное различение людей с похожими чертами лица автоматизированными системами аутентификации усложняется и/или занимает больше времени.

Таким образом, в данной области техники существует потребность в разработке улучшенных автоматизированных систем и способов безопасности для управления доступом к ценностям и ресурсам. В частности, предпочтительно, чтобы автоматизированная система была выполнена с возможностью быстрой и точной аутентификации на основании уникальных личных характеристик, которая может быть легко реализована с возможностью управления доступом к широкому спектру ресурсов и ценностей.

Раскрытие сущности изобретения

Нижеследующие абзацы предназначены для ознакомления читателя с более подробным описанием, которое следует ниже, а не для определения или ограничения заявленного объекта настоящего изобретения.

В одном широком аспекте настоящее изобретение относится к системе безопасности, включающей биометрическую аутентификацию лица. Соответственно, по меньшей мере в одном аспекте настоящего изобретения предложен по меньшей мере один вариант осуществления системы безопасности, содержащей:

устройство управления доступом с электронной блокировкой, выполненное с возможностью разблокировки при аутентификации человека, находящегося перед устройством управления доступом; и

модуль аутентификации, соединенный с устройством управления доступом, содержащий:

устройство для выдачи команд;

камеру, выполненную с возможностью захвата первого изображения лица по меньшей мере части лица человека, находящегося перед камерой; и

центральный контроллер, содержащий процессор и запоминающее устройство, выполненное с возможностью осуществления к нему доступа процессором, причем центральный контроллер соединен с возможностью обмена данными с устройством для выдачи команд и камерой, а запоминающее устройство содержит хранящиеся в нем программные команды, которые при их исполнении процессором конфигурируют центральный контроллер для выполнения первого этапа аутентификации в двухэтапном про-

цессе аутентификации человека, причем первый этап аутентификации включает прием первого маркера аутентификации от человека и аутентификацию первого маркера аутентификации; и выполнения второго этапа аутентификации в двухэтапном процессе аутентификации человека, причем второй этап аутентификации включает:

выбор одной из множества команд по коррекции лица для указания человеку скорректировать по меньшей мере одну черту лица при формировании изображения камерой;

отправку выбранной команды по коррекции лица на устройство для выдачи команд;

выдачу выбранной команды по коррекции лица через устройство для выдачи команд человеку;

захват посредством камеры второго изображения лица человека, в то время как человек корректирует по меньшей мере одну черту лица в соответствии с переданной командой по коррекции лица;

прием центральным контроллером по меньшей мере части второго изображения лица, содержащего по меньшей мере одну скорректированную черту лица человека; и

аутентификацию человека, если часть второго изображения лица совпадает с соответствующим хранимым авторизованным скорректированным изображением лица человека, полученным из хранилища данных скорректированных изображений лица человека; и

разблокирования устройства управления доступом при успешной аутентификации на первом и втором этапах аутентификации.

По меньшей мере в одном варианте осуществления второй этап аутентификации может выполняться только при успешной аутентификации на первом этапе.

По меньшей мере в одном варианте осуществления камера выполнена с возможностью захвата и приема первого маркера аутентификации.

По меньшей мере в одном варианте осуществления модуль аутентификации может содержать дополнительное устройство, которое выполнено с возможностью приема первого маркера аутентификации и которое представляет собой устройство, отличное от камеры.

По меньшей мере в одном варианте осуществления центральный контроллер может быть связан с возможностью обмена данными с хранилищем данных, содержащим множество хранимых в нем авторизованных маркеров аутентификации, первый этап аутентификации включает выполнение сопоставления между принятым маркером аутентификации и хранимыми авторизованными маркерами аутентификации, причем каждый хранимый авторизованный маркер аутентификации связан с хранимыми авторизованными изображениями лица, содержащими скорректированные черты лица человека, а центральный контроллер выполнен с возможностью осуществления аутентификации на втором этапе аутентификации путем выполнения сопоставления исключительно между захваченным скорректированным изображением лица и одним из хранимых авторизованных изображений лица, которые связаны с первым маркером аутентификации и содержат скорректированные черты лица человека.

По меньшей мере в одном варианте осуществления центральный контроллер выполнен с возможностью поиска хранимых авторизованных изображений лица, которые имеют одну или более коррекций лица, которые соответствуют одной или более коррекциям лица в выданной команде по коррекции лица.

По меньшей мере в одном варианте осуществления первый маркер аутентификации может содержать 1D или 2D штрих-код.

По меньшей мере в одном варианте осуществления первый маркер аутентификации может содержать первое изображение лица, захваченное камерой, а аутентификация может включать выполнение сопоставления между захваченным первым изображением лица и хранилищем данных, содержащем хранимые в нем авторизованные изображения лица.

По меньшей мере в одном варианте осуществления камера или устройство для выдачи команд могут быть расположены в непосредственной близости от устройства управления доступом с электронной блокировкой.

По меньшей мере в одном варианте осуществления устройство для выдачи команд может быть выполнено с возможностью выдачи визуальных команд или звуковых команд человеку.

По меньшей мере в одном варианте осуществления визуальные команды могут включать анимацию, представляющую скорректированную черту лица.

По меньшей мере в одном варианте осуществления визуальные команды могут включать текстовые команды для человека по коррекции по меньшей мере одной из его черт лица.

По меньшей мере в одном варианте осуществления центральный контроллер может быть выполнен с возможностью выполнения первого и второго этапов аутентификации в разных, соответственно, первом и втором пространствах.

По меньшей мере в одном варианте осуществления электронное устройство управления доступом может содержать первый и второй электронные компоненты управления доступом, причем первый электронный компонент управления доступом разблокируется после успешной аутентификации на первом этапе аутентификации, а второй электронный компонент управления доступом разблокируется после успешной аутентификации на втором этапе аутентификации.

По меньшей мере в одном варианте осуществления центральный контроллер может быть выполнен с возможностью разблокирования устройства управления доступом только в том случае, если первый

и/или второй этапы авторизации также выполняются в выбранное предварительно одобренное время.

По меньшей мере в одном варианте осуществления электронное устройство управления доступом также может включать в себя устройство для измерения температуры, выполненное с возможностью измерения температуры тела человека, причем устройство для измерения температуры соединено с центральным контроллером, а центральный контроллер выполнен с возможностью разблокирования устройства управления доступом, если измеренная температура тела человека находится в заданном диапазоне температуры тела.

По меньшей мере в одном варианте осуществления устройство для измерения температуры может быть выполнено с возможностью измерения температуры тела человека после выполнения первого и второго этапов аутентификации.

По меньшей мере в одном варианте осуществления заданная температура тела может находиться в диапазоне от приблизительно 36,5 до приблизительно 38,5°C.

Еще в одном аспекте настоящее изобретение относится к способам разблокировки электронного устройства управления доступом системы безопасности, содержащей центральный контроллер. Соответственно, по меньшей мере в одном аспекте настоящего изобретения предложен реализуемый на компьютере способ разблокировки электронного устройства управления доступом системы безопасности, включающий:

захват с помощью камеры изображения лица человека, находящегося перед камерой, при этом камера расположена рядом с электронным устройством управления доступом;

выполнение первого этапа аутентификации в двухэтапном процессе аутентификации человека, причем первый этап аутентификации включает прием первого маркера аутентификации и аутентификацию человека, пытающегося получить доступ, с использованием первого маркера аутентификации;

выполнение второго этапа аутентификации в двухэтапном процессе аутентификации человека, причем второй этап аутентификации включает:

выбор одной из множества команд по коррекции лица для указания человеку скорректировать по меньшей мере одну черту лица при формировании изображения камерой;

инициирование передачи устройством для выдачи команд выбранной команды по коррекции лица человеку; захват с помощью камеры изображения лица человека, корректирующего по меньшей мере одну черту лица в соответствии с переданной командой по коррекции лица; прием по меньшей мере части второго изображения лица, содержащего скорректированную черту лица; и

аутентификацию, если часть изображения лица совпадает с соответствующей хранимой частью изображения человека из хранилища данных скорректированных изображений лица; и

разблокирование устройства управления доступом при успешной аутентификации человека на первом и втором этапах аутентификации.

По меньшей мере в одном варианте осуществления способ включает выполнение второго этапа аутентификации только при успешной аутентификации на первом этапе.

По меньшей мере в одном варианте осуществления способ включает использование камеры для захвата и приема первого маркера аутентификации.

По меньшей мере в одном варианте осуществления способ включает выполнение первого этапа аутентификации с использованием дополнительного устройства, которое выполнено с возможностью приема первого маркера аутентификации и которое представляет собой устройство, отличное от камеры.

По меньшей мере в одном варианте осуществления первый этап аутентификации может включать выполнение сопоставления между принятым маркером аутентификации и хранимыми авторизованными маркерами аутентификации, причем каждый хранимый авторизованный маркер аутентификации связан с хранимыми изображениями лица, содержащими скорректированные черты лица человека, а аутентификация на втором этапе аутентификации выполняется исключительно на основании сопоставления между захваченным скорректированным изображением лица и одним из хранимых авторизованных изображений лица, которые связаны с первым маркером аутентификации и содержат скорректированные черты лица человека.

По меньшей мере в одном варианте осуществления способ включает поиск хранимых авторизованных изображений лица, которые имеют одну или более коррекций лица, которые соответствуют одной или более коррекциям лица в выданной команде по коррекции лица.

По меньшей мере в одном варианте осуществления первый маркер аутентификации может содержать 1D или 2D штрих-код.

По меньшей мере в одном варианте осуществления первый маркер аутентификации может содержать первое изображение лица, захваченное камерой, а аутентификация может включать выполнение сопоставления между захваченным первым изображением лица и хранилищем данных, содержащем хранимые в нем авторизованные изображения лица.

По меньшей мере в одном варианте осуществления камера или устройство для выдачи команд могут быть расположены в непосредственной близости от устройства управления доступом с электронной блокировкой.

По меньшей мере в одном варианте осуществления способ включает использование устройства для

выдачи команд для выдачи визуальных команд или звуковых команд человеку.

По меньшей мере в одном варианте осуществления визуальные команды могут включать анимацию, представляющую скорректированную черту лица.

По меньшей мере в одном варианте осуществления визуальные команды могут включать текстовые команды для человека по коррекции по меньшей мере одной из его черт лица.

По меньшей мере в одном варианте осуществления первый и второй этапы аутентификации могут выполняться в разных, соответственно, первом и втором пространствах.

По меньшей мере в одном варианте осуществления электронное устройство управления доступом может содержать первый и второй электронные компоненты управления доступом, а способ включает разблокирование первого электронного компонента управления доступом после успешной аутентификации на первом этапе аутентификации и разблокирование второго электронного компонента управления доступом после успешной аутентификации на втором этапе аутентификации.

По меньшей мере в одном варианте осуществления способ включает разблокирование устройства управления доступом только в том случае, если первый и/или второй этапы авторизации также выполняются в выбранное предварительно одобренное время.

По меньшей мере в одном варианте осуществления электронное устройство управления доступом также может включать в себя устройство для измерения температуры, а способ также включает измерение температуры тела человека с помощью устройства для измерения температуры и разблокирование устройства управления доступом, если измеренная температура тела человека находится в заданном диапазоне температуры тела.

По меньшей мере в одном варианте осуществления способ включает использование устройства для измерения температуры для измерения температуры тела человека после выполнения первого и второго этапов аутентификации.

По меньшей мере в одном варианте осуществления заданная температура тела может находиться в диапазоне от приблизительно 36,5 до приблизительно 38,5°C.

Другие признаки и преимущества настоящего изобретения станут понятными из нижеследующего подробного описания. Однако следует понимать, что хотя в подробном описании представлены некоторые варианты реализации настоящего изобретения, они приведены исключительно в качестве иллюстрации, поскольку различные изменения и модификации в рамках сущности и объема настоящего изобретения станут очевидными для специалистов в данной области техники после ознакомления с подробным описанием.

Краткое описание чертежей

Раскрытие изобретения представлено в качестве примера в приведенных ниже абзацах со ссылкой на прилагаемые чертежи. Представленные в настоящем документе чертежи предназначены для лучшего понимания примеров осуществления и более ясной иллюстрации того, как могут быть реализованы различные варианты осуществления. Эти чертежи не предназначены для ограничения настоящего изобретения.

На фиг. 1 представлен схематический вид системы безопасности, содержащей электронное устройство управления доступом согласно приведенному в качестве примера варианту осуществления настоящего изобретения.

На фиг. 2 представлен схематический вид устройства управления доступом с электронной блокировкой согласно приведенному в качестве примера варианту осуществления настоящего изобретения.

На фиг. 3A, 3B представлено изображение лица (фиг. 3A) и изображение лица, содержащее скорректированные черты лица (фиг. 3B), согласно приведенному в качестве примера варианту осуществления настоящего изобретения.

На фиг. 4 представлен схематический вид маркеров аутентификации, которые хранятся в хранилище данных, согласно одному аспекту приведенного в качестве примера варианта осуществления настоящего изобретения.

На фиг. 5 представлена блок-схема способа разблокирования устройства управления доступом с электронной блокировкой системы безопасности согласно приведенному в качестве примера варианту осуществления настоящего изобретения.

На фиг. 6 представлен еще один пример осуществления системы безопасности, содержащей электронное устройство управления доступом, в соответствии с изложенными в настоящем документе идеями.

Осуществление изобретения

Далее будут описаны различные системы и процессы в качестве примера реализации или осуществления каждого заявленного объекта изобретения. Ни один из вариантов реализации или осуществления, описанных ниже, не ограничивают любой из заявленных объектов и любой из заявленных объектов может охватывать способы, системы, устройства, сборки, процессы или аппараты, которые отличаются от описанных ниже. Заявленный объект изобретения не ограничивается системами или процессами, имеющими все признаки любой одной системы, способа, устройства, аппарата, узла или процесса, описанных ниже, или признаками, общими для множества или всех систем, способов, устройств, аппаратов, узлов

или процессов, описанных ниже. Возможно, что система или процесс, описанные ниже, не являются вариантом реализации или осуществления какого-либо из заявленных объектов изобретения. Любой объект, раскрытый в системе или процессе, описанных ниже, который не заявлен в настоящем документе, может представлять собой объект другого документа, находящегося под правовой охраной, например, продолжающейся патентной заявки, и заявители, авторы изобретения или его владельцы не намерены уступать или открывать кому-либо любой такой объект или отказываться от него, раскрывая его в этом документе.

Используемые в описании и формуле изобретения грамматические средства выражения формы единственного числа включают множественное число и наоборот, если контекст явно не указывает на иное. В настоящем описании, если не указано иное, термины "содержать", "содержит" и "содержащий" используются скорее включительно, чем исключительно, так что указанное целое число или группа целых чисел может включать в себя одно или более других неуказанных целых чисел, либо одну или более групп целых чисел.

Термин "или" является включающим, если только он не включен, например, в грамматическую конструкцию, соответствующую "исключающему или".

Если в настоящем документе используются диапазоны, например, для геометрических параметров, например расстояний, в них включены все комбинации и подкомбинации диапазонов и конкретные варианты реализации в них. За исключением рабочих примеров или если указано иное, все числа, выражающие количества ингредиентов или условия реакции, используемые в настоящем документе, следует понимать как измененные во всех случаях термином "приблизительно".

Термин "приблизительно" в отношении числа или числового диапазона означает, что указанное число или числовой диапазон являются приблизительными в пределах колебания показаний от эксперимента к эксперименту (или в пределах статистической экспериментальной ошибки), и, таким образом, число или числовой диапазон могут варьироваться в пределах от 1 до 15% от указанного числа или числового диапазона, что можно будет легко понять из контекста. Кроме того, любой диапазон значений, описанный в настоящем документе, определенно предназначен для включения ограничивающих значений диапазона и любого промежуточного значения или поддиапазона в пределах данного диапазона и все такие промежуточные значения и поддиапазоны раскрыты по отдельности и конкретно (например, диапазон от 1 до 5 включает 1, 1,5, 2, 2,75, 3, 3,90, 4 и 5).

Аналогичным образом, другие термины для указания степени, такие как "по существу" и "приблизительно", используемые в настоящем документе для изменения термина, следует понимать как означающие приемлемую величину отклонения измененного термина, которое существенно не изменяет конечный результат. Эти термины для указания степени следует истолковывать как включающие отклонение от измененного термина, если это отклонение не отменяет значение термина, который он изменяет.

Если не указано иное, научные и технические термины, используемые в связи с описанными в настоящем документе формулировками, имеют значения, которые обычно понятны специалистам в данной области. Используемая в настоящем документе терминология предназначена исключительно для описания конкретных вариантов реализации и не предназначена для ограничения объема настоящего изобретения, которое определяется исключительно формулой изобретения.

Все публикации, патенты и патентные заявки включены в данный документ посредством ссылки в том же объеме, как если бы каждая отдельная публикация, патент или патентная заявка были специально и по отдельности указаны как включенные посредством ссылки в полном объеме.

Определения

Термины "автоматизированная система" или "система", взаимозаменяемо используемые в настоящем документе, относятся к устройству или конфигурации множества устройств с одним или более электронными обрабатывающими элементами, способными выполнять машинно-исполняемые программные команды, причем эти устройства включают, без ограничений, любой персональный компьютер, настольный компьютер, карманный компьютер, портативный планшетный компьютер, компьютер сотового телефона, компьютер смартфона или другое подходящее электронное устройство или множество устройств.

Часть примеров осуществления систем, устройств или способов, описанных в настоящем документе в соответствии с идеями настоящего изобретения, может быть реализована в виде комбинации аппаратного или программного обеспечения. Например, часть описанных в настоящем документе вариантов осуществления может быть реализована, по меньшей мере частично, с использованием одной или более компьютерных программ, исполняемых на одном или более программируемых устройствах, каждое из которых содержит по меньшей мере один обрабатывающий элемент и по меньшей мере один элемент для хранения данных (включая запоминающее устройство для кратковременного и долговременного хранения данных). Эти устройства также могут содержать по меньшей мере одно устройство ввода и по меньшей мере одно устройство вывода, как определено в настоящем документе.

Следует также отметить, что могут присутствовать некоторые элементы, используемые для реализации по меньшей мере части описанных в настоящем документе вариантов осуществления, которые могут быть реализованы с помощью программного обеспечения, написанного на процедурном языке

высокого уровня, например, с применением объектно-ориентированного программирования. Программный код может быть написан на MATLAB™, Visual Basic, Fortran, C, C^{++} или любом другом подходящем языке программирования и может содержать модули или классы, известные специалистам по объектно-ориентированному программированию. В качестве альтернативы или в дополнение к этому некоторые из этих элементов, реализованных с помощью программного обеспечения, могут быть при необходимости написаны на языке ассемблера, машинном языке или в виде встраиваемого программного обеспечения.

По меньшей мере некоторые из программных продуктов, используемых для реализации по меньшей мере одного из описанных в настоящем документе вариантов осуществления, могут храниться на носителе данных (например, машиночитаемом носителе, таком как, без ограничений, ПЗУ, магнитный диск, оптический диск) или устройстве, выполненном с возможностью считывания с помощью универсального или специализированного программируемого устройства. Программный код при его считывании по меньшей мере одним процессором программируемого устройства конфигурирует по меньшей мере один процессор для работы новым, специфическим и заранее определенным способом для выполнения по меньшей мере одного из способов, описанных в настоящем документе.

Кроме того, по меньшей мере некоторые из программ, связанных с системами и способами согласно вариантам осуществления, описанными в настоящем документе, могут быть выполнены с возможностью распространения в компьютерном программном продукте, включающем в себя машиночитаемый носитель, который содержит используемые на компьютере/считываемые с помощью компьютера команды, такие как программный код или программные команды, для одного или более процессоров. Программный код может быть предварительно установлен и встроен во время производства и/или может быть установлен позже в виде обновления на уже развернутой вычислительной системе.

Носитель может иметь различные формы, включая энергонезависимые формы, такие как, без ограничений, одна или более дискет, компакт-дисков, лент, микросхем, USB-ключей, внешних жестких дисков, магнитных и электронных носителей данных, планшетов (например, iPad) или приложений для смартфонов (например, iPhone), аппаратов и т.п. В альтернативных вариантах осуществления среда может быть энергозависимой по своей природе, например, без ограничений, она может представлять собой проводные передачи, спутниковые передачи, Интернет-передачи (например, загрузки), среды, а также цифровые и аналоговые сигналы. Используемые на компьютере команды также могут иметь различные форматы, включая скомпилированный и нескомпилированный код.

Используемый в настоящем документе термин "соединенный" может иметь несколько различных значений в зависимости от контекста, в котором используется этот термин. Например, термин "соединенный" может иметь механический или электрический оттенок значения в зависимости от контекста, в котором он используется, т.е. от того, описывается ли схема расположения или передача данных, в каждом конкретном случае. Например, в зависимости от контекста, термин "соединенный" может указывать на то, что два элемента или устройства могут быть непосредственно физически или электрически соединены друг с другом или соединены друг с другом через один или более промежуточных элементов или устройств посредством физического или электрического элемента, такого как, без ограничений, например, провод, неактивный элемент схемы (например, резистор) и т.п.

Термин "устройство ввода", используемый в настоящем документе, относится к любому устройству, управляемому пользователем, которое используют для ввода информации и которое включает, без ограничений, один или более терминалов, сенсорный экран, клавиатуру, мышь, планшет мыши, шаровой манипулятор, джойстик, микрофон, систему распознавания голоса, световое перо, камеру, устройство ввода данных, такое как считыватель штрих-кода или устройство для распознавания знаков, написанных магнитными чернилами, датчик или любой другой вычислительный блок, выполненный с возможностью приема входных данных. В некоторых вариантах осуществления устройства ввода могут содержать двумерный дисплей, такой как телевизор или жидкокристаллический дисплей (ЖКД), дисплей с подсветкой на светодиодах (light-emitting diode, LED) или дисплей мобильного телефона, выполненный с возможностью приема данных, введенных пользователем, например сенсорный экран. Пользователь в соответствии с настоящим документом может быть любым пользователем или оператором, включая, например, любого менеджера по безопасности, оператора или менеджера на месте выполнения работ.

Термин "устройство вывода", используемый в настоящем документе, относится к любому устройству, используемому для вывода информации, и включает, без ограничений, один или более дисплейных терминалов, экран, принтер (например, лазерный, струйный, матричный), плоттер или другое устройство для выдачи документальных копий, динамик, наушники, электронное запоминающее устройство, радиооборудование или другое устройство связи, выполненное с возможностью обмена данными с другим устройством, или любой другой вычислительный блок. Устройства вывода также могут включать двумерный дисплей, такой как телевизор или жидкокристаллический дисплей (ЖКД), дисплей с подсветкой на светодиодах (light-emitting diode, LED) и/или дисплей мобильного телефона, выполненный с возможностью отображения выходных данных пользователю в наглядном формате.

Общая реализация системы.

Как упоминалось выше, настоящее изобретение относится к автоматизированным системам безопасности и связанным с ними процессам, включающим биометрическую аутентификацию. Автоматизи-

рованная система безопасности и связанные с ней процессы могут быть реализованы с возможностью управления доступом к ценным ресурсам с помощью блокируемого устройства управления доступом таким образом, чтобы только авторизированные лица могли получить доступ посредством блокируемого устройства управления доступом. В частности, система и процессы согласно настоящему изобретению включают аутентификацию на основе биометрической информации о лице. Система может быть выполнена с возможностью идентификации злоумышленников или хакеров, представляющих копии аутентифицированных изображений лица, например, их фотографий, и может отказать в доступе таким злоумышленникам или хакерам. Кроме того, настоящая система может быть выполнена с возможностью сокращения количества вычислительных операций, требуемых для выполнения этапа распознавания лица, и/или сокращения количества ошибок при аутентификации людей с аналогичными чертами лица. Эти и другие предпочтительные аспекты делают описанную в настоящем документе систему полезной для защиты ценных ресурсов от несанкционированного доступа к ним.

Соответственно, по меньшей мере в одном аспекте настоящего изобретения предложен по меньшей мере один вариант осуществления системы безопасности, содержащей:

устройство управления доступом с электронной блокировкой, выполненное с возможностью разблокировки при аутентификации человека, находящегося перед устройством управления доступом; и

модуль аутентификации, соединенный с устройством управления доступом, содержащий:

устройство для выдачи команд;

камеру, выполненную с возможностью захвата по меньшей мере части изображения лица человека, расположенного перед камерой; и

центральный контроллер, содержащий процессор и запоминающее устройство, выполненное с возможностью осуществления к нему доступа процессором, причем центральный контроллер соединен с возможностью обмена данными с устройством для выдачи команд и камерой, а запоминающее устройство содержит программные команды, хранящиеся в нем, которые при их исполнении процессором конфигурируют центральный контроллер для выполнения первого этапа аутентификации в двухэтапном процессе аутентификации человека, причем первый этап аутентификации включает:

прием первого маркера аутентификации и аутентификацию первого маркера аутентификации; и выполнения второго этапа аутентификации в двухэтапном процессе аутентификации человека, причем второй этап аутентификации включает:

выбор одной из множества команд по коррекции лица для указания человеку скорректировать по меньшей мере одну черту лица при формировании изображения камерой;

отправку выбранной команды по коррекции лица на устройство для выдачи команд;

передачу выбранной команды по коррекции лица через устройство для выдачи команд человеку;

захват с помощью камеры изображения лица человека, корректирующего по меньшей мере одну черту лица в соответствии с переданной командой по коррекции лица;

прием центральным контроллером по меньшей мере части изображения лица, содержащего по меньшей мере одну скорректированную черту лица человека; и

аутентификацию человека, если часть изображения лица совпадает с соответствующей хранимой частью изображения человека из хранилища данных скорректированных изображений лица человека; и

разблокирования устройства управления доступом при успешной аутентификации на первом и втором этапах аутентификации.

Пример осуществления системы безопасности согласно настоящему изобретению показан на фиг. 1. Таким образом, как показано на фиг. 1, в примере осуществления настоящего изобретения предложена система 100 безопасности для ограничения доступа в рабочее пространство 115, огороженное забором 110 или другим ограждением от наружного пространства 117. В рабочем пространстве 115 находятся некоторые производственные ценности, а именно ручные тележки 107a и 107b, а также вычислительное устройство 106. Следует отметить, что пространство, представленное в качестве примера как рабочее пространство 115, в котором находятся ценности, представленные в качестве примера в виде ручных тележек 107a и 107b и вычислительного устройства 106, согласно различным вариантам осуществления настоящего изобретения может представлять собой любое пространство, для которого требуется контроль доступа, включая любое рабочее пространство или любое частное пространство, включая частное домашнее пространство. Кроме того, ценности могут представлять собой любые физические ценности, такие как, например, оборудование, документы или денежная валюта. Ценности также могут представлять собой электронную информацию, например, личную информацию, банковскую информацию, электронную информацию о профиле пользователя и т.д. Рабочее пространство 115 может представлять собой физическое пространство, такое как, без ограничений, здание или территория, например, которая может быть огорожена от наружного пространства 117 любой конструкцией с ограничением доступа, определяющей периметр пространства, такой как стена, забор, заграждение, перильное ограждение, живая изгородь или любая другая ограждающая конструкция. В других вариантах осуществления рабочее пространство 115 также может представлять собой виртуальное пространство, например, электронный домен или пространство, содержащее информацию, к которой можно осуществить доступ посредством устройства ввода, такого как компьютерный терминал. Таким образом, например, рабочее

пространство 115 в некоторых вариантах осуществления может представлять собой компьютерный домен, содержащий электронную банковскую информацию человека, доступ к которой человек запрашивает через банкомат. Следует понимать, что настоящее изобретение не ограничено конкретным пространством, рабочим пространством или частным пространством, либо конкретными ценностями, содержащимися в нем и доступными с использованием системы безопасности согласно настоящему изобретению. Система безопасности согласно настоящему изобретению может быть реализована в любом пространстве и для любых ценностей, содержащихся в нем.

Как также показано на фиг. 1, люди 105a и 105b получили доступ в рабочее пространство 115 из наружного пространства 117 через открываемые ворота 215 с электронным замком. В этом отношении открываемые ворота 215 являются частью устройства 200 управления доступом с электронным замком. Запиранием и отпиранием открываемых ворот 215 управляет модуль 109 аутентификации, содержащий центральный контроллер 145, камеру 205 и устройство 210 для выдачи команд, как далее будет более подробно описано со ссылкой на фиг. 2. Центральный контроллер 145 представляет собой сервер, содержащий процессор и запоминающее устройство, в котором хранятся программные команды. Центральный контроллер 145 электронным способом соединен с устройством 200 управления доступом с электронным замком посредством сети 130. Модуль 109 аутентификации также содержит устройство 140 ввода и устройство 150 вывода, каждое из которых соединено с центральным контроллером 145 для, соответственно, обеспечения ввода данных в центральный контроллер 145 и таким образом управления центральным контроллером 145, а также приема выходного сигнала от центрального контроллера 145, если это необходимо оператору центрального контроллера 145.

Центральный контроллер 145 содержит любой подходящий компьютерный процессор, который способен обеспечить достаточную вычислительную мощность в зависимости от требований центрального контроллера 145, как известно специалистам в данной области техники. Центральный контроллер 145 может включать в себя один процессор. В качестве альтернативы, может применяться множество процессоров, используемых центральным контроллером 145, которые могут работать параллельно и выполнять определенные функции. В альтернативных вариантах осуществления для осуществления некоторых из функций, обеспечиваемых центральным контроллером 145, может использоваться специализированное оборудование.

Центральный контроллер 145 может включать в себя порты и/или устройства, с помощью которых центральный контроллер 145 может обмениваться данными с другими устройствами или компьютерами. В некоторых случаях они могут включать по меньшей мере один из последовательного порта, параллельного порта или порта универсальной последовательной шины (Universal Serial Bus, USB), которая обеспечивает подключение по USB. Центральный контроллер 145 также может иметь соединение по меньшей мере с одним из Интернета, локальной сети (Local Area Network, LAN), Ethernet, Firewire, модема или цифровой абонентской линии. Например, центральный контроллер 145 может включать в себя стандартный сетевой адаптер, такой как адаптер Ethernet или 802.11x. В некоторых вариантах осуществления центральный контроллер 145 может включать в себя радиомодуль, выполненный с возможностью обмена данными с использованием протокола CDMA, GSM, GPRS или Bluetooth в соответствии со такими стандартами, как IEEE 802.11a, 802.11b, 802.11g или 802.11n. Различные комбинации этих элементов могут быть встроены в центральный контроллер 145 или могут использоваться ним.

Хранилище 114 данных, которое включено в центральный контроллер 145, может включать ОЗУ, ПЗУ, один или более жестких дисков, один или более флэш-накопителей или некоторые другие подходящие элементы для хранения данных, такие как дисковые накопители и т. д. Хранилище 114 данных может хранить программные команды для операционной системы, программный код для различных приложений и одну или более баз данных. Программы содержат программный код, при исполнении которого происходит конфигурирование центрального контроллера 145 для обеспечения его работы определенным образом для реализации различных функций, инструментов, процессов и способов для функционирования системы 100 безопасности. Например, программный код может включать в себя программные команды для выполнения различных способов в соответствии с изложенными в настоящем документе идеями, примеры которых показаны на фиг. 5. Хранилище 114 данных также может хранить различные рабочие параметры, маркеры аутентификации и/или результаты аутентификации. В некоторых вариантах осуществления хранилище 114 данных может представлять собой отдельное устройство, выполненное с возможностью удаленного доступа к нему центрального контроллера 145, при этом некоторые элементы, которые были описаны ранее как хранящиеся в хранилище 114 данных, альтернативно или дополнительно могут храниться в запоминающем устройстве центрального контроллера 145.

Рассмотрим фиг. 2 и 3A, 3B. На фиг. 2 показано устройство 200 управления доступом с электронным замком, расположенное по периметру рабочего пространства 115 и отделяющее рабочее пространство 115 от наружного пространства 117. Устройство 200 управления доступом с электронным замком содержит открываемые ворота 215, имеющие поворотный элемент 217 в виде петли ворот и опорные конструкции 216a, 216b ворот. Как уже отмечалось, устройство 200 управления доступом с электронным замком соединено с центральным блоком 145 управления посредством сети 130. Чтобы перевести открываемые ворота 215 из заблокированного и закрытого положения, как показано на фиг. 1, в открытое по-

ложение, как показано на фиг. 2, центральный контроллер 145 может передать сигнал на устройство 200 управления доступом для разблокировки элементов 230a и 230b для электронной блокировки, которые могут, например, представлять собой элементы для электромагнитной блокировки, вместе образуя электронный замок 230, что позволяет открывать или закрывать открываемые ворота 215.

Система 100 безопасности также выполнена таким образом, что после успешной аутентификации человека, желающего получить доступ в рабочее пространство 115 из наружного пространства 117 через проход 119, открываемые ворота 215 разблокируются. Когда открываемые ворота 215 открывается из закрытого положения (показанного на фиг. 1), образуется проход 119, как показано на фиг. 2. Таким образом, другими словами, система 100 безопасности выполнена таким образом, что в ней требуется аутентификация человека, желающего получить доступ в рабочее пространство 115 из наружного пространства 117, перед предоставлением доступа в рабочее пространство 115. Таким образом, доступом в рабочее пространство 115 может управлять и ограничивать его владелец или оператор системы 100 безопасности. Это включает предоставление доступа в рабочее пространство 115 определенным лицам и запрет на доступ другим лицам, а также предоставление доступа в рабочее пространство 115 определенным лицам на определенный период времени и запрет на такой доступ другим лицам, например, доступ в рабочее пространство 115 на конкретную неделю или доступ в рабочее пространство 115 только в дневное время, как описано ниже.

Система 100 безопасности также выполнена с возможностью выполнения двухэтапного процесса аутентификации. Сначала человек, желающий получить доступ в рабочее пространство 115, подходит к открываемым воротам 215, которые закрыты в заблокированном положении. Затем человек представляет первый маркер аутентификации.

Термин "маркер аутентификации", используемый в настоящем документе, относится к физическому объекту, который содержит любой набор признаков, включая биометрические признаки, и содержится на любом носителе, который выполнен с возможностью его приема системой безопасности с целью идентификации представившего его человека. Первый маркер аутентификации в некоторых вариантах осуществления представляет собой идентификационную карту, например, идентификационную карту, содержащую одномерный (1-dimensional, 1D) линейный штрих-код или двухмерный (two-dimensional, 2D) штрих-код, например QR-код, DataMatrix или PDF417. Такие штрих-коды в соответствующих случаях могут включать коды с исправлением ошибок, такие как, например, коды на основе прямого исправления ошибок (forward error correction, FEC) или коды на основе принципа Рида-Соломона.

Как также показано на фиг. 1 и 2, вся информация (или ее часть) о первом маркере аутентификации предъявляется на камеру 205, установленную рядом с открываемыми воротами 215, и захватывается ней. В этом отношении следует отметить, что камеру 205 предпочтительно устанавливать в пределах метров или десятков метров от открываемых ворот 215. В некоторых вариантах осуществления камера 205, а также устройство 210 для выдачи команд (которое, как обсуждается ниже, также устанавливают рядом с открываемыми воротами 215) встроены в конструкцию, содержащую открываемые ворота 215, например, размещены внутри нее или прикреплены к опорным конструкциям 216a, 216b ворот. В других вариантах осуществления для представления первого маркера аутентификации может использоваться еще одна камера или другое устройство, выполненные с возможностью приема первого маркера аутентификации, например, сканер, расположенный в непосредственной близости от открываемых ворот 215. Как будет очевидно далее, устройство, используемое для приема первого маркера аутентификации, выбирают таким образом, чтобы оно было совместимо с форматом первого маркера аутентификации, т. е. это устройство должно быть выполнено с возможностью получения соответствующей информации для целей аутентификации из первого маркера аутентификации, причем оно может варьироваться в зависимости от физической природы выбранного первого маркера аутентификации (например, от того, является ли маркер идентификационной картой со штрих-кодом на ее поверхности или идентификационной картой, в которую встроен чип, содержащий штрих-код, или другим средством, содержащим идентификационные данные). Таким образом, устройство может представлять собой сканер, считыватель для микросхем, камеру или т. п., выбранные для соответствия формату первого маркера аутентификации для его получения.

По меньшей мере в одном варианте осуществления первый маркер аутентификации содержит биометрические признаки, включая, например, отпечатки пальцев или биометрические признаки лица. Такие биометрические признаки могут быть захвачены в виде визуального изображения, например, изображения лица человека, предъявляющего первый маркер аутентификации. В этом отношении термин "изображение лица" означает изображение всего лица человека или его части. Как показано на фиг. 1 и 2, изображение лица может быть захвачено камерой 205 после того, как человек окажется в пределах пространства 117b для представления. Это изображение лица можно назвать первым маркером аутентификации. Следует отметить, что в некоторых вариантах осуществления человек может инициировать первый этап аутентификации, выполнив действие, например нажав кнопку активации, соединенную с камерой 205 и, например, установленную в непосредственной близости от камеры 205, чтобы, таким образом, инициировать захват камерой 205 изображения лица находящегося перед ней человека. В других вариантах осуществления камера 205 может содержать датчик, выполненный с возможностью обнаружения

перемещения человека в пространстве 117b для представления, и камера 205 может автоматически захватывать изображение лица при обнаружении человека в пространстве 117b для представления. В этом случае захваченное изображение лица является первым маркером аутентификации.

Камера 205 передает захваченный первый маркер аутентификации в центральный контроллер 145. Центральный контроллер 145 выполнен с возможностью осуществления доступа к хранимым маркерам аутентификации всех лиц, имеющих авторизованный доступ в рабочее пространство 115, в хранилище 114 данных компонента-запоминающего устройства. Хранимые маркеры аутентификации могут быть введены для хранения в хранилище 114 данных компонента-запоминающего устройства центрального контроллера 145 через устройство 140 ввода, которым управляет, например, оператор-администратор системы 100 безопасности. После такого ввода указанных маркеров аутентификации в хранилище 114 данных эти маркеры авторизации становятся хранимыми авторизованными маркерами аутентификации. Таким образом, хранилище 114 данных может быть выполнено с возможностью хранения множества сохраненных авторизованных маркеров аутентификации и может содержать, например, сотни, тысячи, десятки тысяч или более хранимых авторизованных маркеров аутентификации. Таким образом, со ссылкой на фиг. 1 также отметим, что отдельные маркеры аутентификации для рабочих 105a и 105b могут храниться в хранилище 114 данных. В базе 114 данных хранимые маркеры аутентификации, как правило, предпочтительно связаны с личной информацией, например именами, датами рождения, телефоном и т. д., рабочих 105a и 105b. Это позволяет владельцу или оператору системы безопасности 100 идентифицировать работника 105a и 105b, например, в том случае, если доступ к пространству 115 запрещен, и рабочий 105a или 105b, либо владелец или оператор системы 100 безопасности желают выяснить причину отказа в доступе.

Для выполнения первого этапа аутентификации центральный контроллер 145 выполнен с возможностью сравнения первого маркера аутентификации, захваченного от человека, который находится в пространстве 117b для представления, с авторизованными маркерами аутентификации, хранимыми в хранилище 114 данных. В этом отношении, в зависимости от формата захваченного первого маркера аутентификации различные признаки с первого маркера аутентификации могут быть сравнены с признаками, присутствующими в хранилище 114 данных. Например, в вариантах осуществления настоящего изобретения, в которых в качестве маркеров аутентификации используются 1D или 2D штрих-коды, признаки представленных штрих-кодов, включая визуальные узоры (например, для 1D штрих-кодов: количество полос, размер полос, относительное расстояние между полосами) сравнивают с признаками штрих-кодов хранимых авторизованных маркеров аутентификации. Центральный контроллер 145 выполнен с возможностью идентификации штрих-кода в хранимом авторизованном маркере аутентификации в хранилище 114 данных с признаками, идентичными признакам представленных штрих-кодов, и, таким образом, устанавливать соответствие между двумя штрих-кодами. Машинно-исполняемый программный код для конфигурирования центрального контроллера 145 в этом отношении хорошо известен специалистам в данной области техники и включает, например, программное обеспечение для сканирования штрих-кодов Google® ZXing (http://code.google.com/p/zxing/), Apple® Scan для iPhone, Optiscan, QRafter, ScanLife, I-Nigma, Quickmark, Kaywa Reader, Nokia® Barcode Reader, Blackberry® Messenger, Esponce® QR Reader и/или т.п.

В вариантах осуществления настоящего изобретения, в которых первый маркер аутентификации содержит захваченное изображение лица или его часть, первый этап аутентификации включает идентификацию возможного соответствия между захваченным изображением лица и хранимыми авторизованными маркерами аутентификации, включающими в себя изображения лиц, которые хранятся в хранилище 114 данных, на основании различимых черт лица. Такое соответствие может быть основано на геометрической форме лица, например, как показано на фиг. 3A, которая может включать, без ограничений, один из следующих параметров: межзрачковое расстояние d1 между зрачком 310 правого глаза и зрачком 305 левого глаза, расстояние d2 между зрачком 310 правого глаза и кончиком 315 носа, расстояние d3 между кончиком 315 носа и губами 320, а также угол a1, образованный отрезками d1 и d2, которые представляют собой примеры геометрических форм, определяющих, например, черты лица. Другие подходящие способы и технологии, позволяющие выполнять идентификацию на основании соответствия между представленными чертами лица в захваченном изображении и чертами лица в хранимом изображении, известны в данной области техники и включают, например, способы и технологии, описанные в патенте США № 8406484, который включен в настоящий документ посредством ссылки. Кроме того, сопоставление характеристик лица с образцом на основе нейронной сети может использоваться либо отдельно, либо в комбинации с сопоставлением на основе геометрической формы лица (см., например, патент США № 10333714, который включен в настоящий документ посредством ссылки).

При отсутствии соответствия между хранимыми авторизованными маркерами аутентификации и первым маркером аутентификации доступ запрещается, и открываемые ворота 215 остаются закрытыми в заблокированном положении. Если, с другой стороны, установлено соответствие между хранимым авторизованным маркером аутентификации и первым маркером аутентификации, центральный контроллер 145 выполняет второй этап аутентификации, который включает передачу команды по коррекции ли-

ца на устройство 210 для выдачи команд, которое, в свою очередь, передает команду по коррекции лица человеку, пытающемуся получить доступ.

Устройство 210 для выдачи команд, которое, как и камера 205, установлено рядом с открываемыми воротами 215, может представлять собой любое устройство, выполненное с возможностью передачи команды по коррекции лица человеку, пытающемуся получить доступ, включая визуальную или звуковую команду, и содержит, например, двумерный дисплей, ЖК-дисплей, например, или динамик. Визуальные команды включают в себя текстовые команды или команды на основе изображений, например, команду в виде анимации, например, показанную на фиг. 3B, которая представляет собой изображение, используемое для указания человеку 301 закрыть левый глаз 305. Такая команда по коррекции лица предпочтительно выбирается случайным образом из множества возможных команд по коррекции лица для коррекции одной или более черт лица человека, пытающегося получить доступ, на втором этапе аутентификации. К этим командам относятся, например, команда по коррекции лица, указывающая закрыть правый глаз, закрыть левый глаз, открыть рот, нахмурить брови, улыбнуться и т. д. Затем камера 205 захватывает изображение лица человека, пытающегося получить доступ, содержащее по меньшей мере одну скорректированную черту лица, в соответствии с командой по коррекции лица. После захвата изображения камера 205 передает захваченное изображение лица, содержащее по меньшей мере одну скорректированную черту лица, в центральный контроллер 145. Центральный контроллер 145 может осуществить доступ к хранилищу 114 данных, в котором хранятся авторизованные изображения лица, содержащие по меньшей мере одну скорректированную черту лица человека. На этом этапе аутентификации центральный контроллер 145 сравнивает захваченное изображение, содержащее по меньшей мере одно скорректированное изображение лица, например, изображение человека, пытающегося получить доступ, с закрытым левым глазом, с хранимыми авторизованными изображениями скорректированных изображений черт лица человека, пытающегося получить доступ. При отсутствии соответствия доступ запрещается и открываемые ворота 215 остаются закрытыми в заблокированном положении. При установлении соответствия между одним из хранимых авторизованных изображений лица, содержащих по меньшей мере одну скорректированную черту лица, и захваченным изображением лица, содержащим по меньшей мере одну скорректированную черту лица, центральный контроллер 145 передает сигнал для разблокировки электронного замка 230, таким образом, разрешая открыть ворота 215 и позволяя человеку получить доступ в рабочее пространство 115. Следует отметить, что в некоторых вариантах осуществления может передаваться множество команд по коррекции лица для отображения скорректированных черт лица, например, нахмурить брови, закрыть левый глаз, что приведет к выполнению двух или более (т.е. N) вторых этапов аутентификации. В этом случае второй этап аутентификации выполняется N раз и второй этап аутентификации является успешным, если N захваченных изображений, содержащих по меньшей мере одну скорректированную черту лица человека, пытающегося получить доступ, соответствуют N хранимым авторизованным изображениям лица, содержащим по меньшей мере одну скорректированную черту лица человека, пытающегося получить доступ.

По меньшей мере в одном варианте осуществления авторизованные хранимые изображения лица, содержащие скорректированные черты лица, связаны с первым хранимым маркером аутентификации в хранилище 114 данных, как дополнительно проиллюстрировано на фиг. 4. На фиг. 4 представлен схематический обзор хранимых в хранилище 405 данных аутентификационной информации, относящейся к человеку 410 и человеку 415. Штрих-код 410c, представляющий хранимый авторизованный маркер аутентификации, соответствующий первому маркеру аутентификации, связан с авторизованными изображениями лица, содержащими скорректированные черты лица 410a и 410b, представляющие скорректированные черты лица человека 410 (левый глаз закрыт на изображении 410a лица; и нахмуренные брови на изображении 410b лица). Штрих-код 410c и авторизованные изображения 410a и 410b лица содержатся в записи 405a хранилища данных. Штрих-код 415c, представляющий еще один хранимый авторизованный маркер аутентификации, соответствующий первому маркеру аутентификации, связан с авторизованными изображениями лица, содержащими скорректированные черты 415a и 415b лица человека 415 (левый глаз закрыт на изображении 415a лица; и нахмуренные брови на изображении 415b лица). Штрих-код 410c и авторизованные изображения 410a и 410b лица содержатся в записи 405b хранилища данных.

Центральный контроллер 145 выполнен с возможностью выполнения второго этапа аутентификации путем сравнения принятого изображения лица, содержащего скорректированные черты лица человека 410, только с хранимыми авторизованными изображениями 410a и 410b лица, содержащими скорректированные черты лица, связанные со штрих-кодом 410c, а не с хранимыми авторизованными изображения 415a и 415b лица, содержащими скорректированные черты лица, связанные со штрих-кодом 415c, или другими хранимыми авторизованными изображениями лица, содержащими скорректированные черты лица (не показаны). В одном примере осуществления центральный контроллер 145 выполнен с возможностью осуществления второго этапа аутентификации путем сравнения принятого изображения лица только с хранимым авторизованным изображением лица, содержащим скорректированные черты лица, в котором коррекции лица соответствуют одной или более командам по коррекции лица, которые выдаются устройством 210 для выдачи команд человеку, который пытается пройти авторизацию. Таким образом, например, если устройство 210 для выдачи команд выдало команду по коррекции лица человеку 410

с указанием скорректировать черту лица, закрыв левый глаз, центральный контроллер 145 выполняет поиск авторизованных изображений 410a и 410b лица. Затем центральный контроллер 145 идентифицирует изображение 410a лица как соответствующее команде по коррекции лица и сравнение между захваченным изображением и авторизованным изображением лица, содержащим скорректированные черты 410a и 410b лица, выполняется только с использованием авторизованного изображения 410a лица, но не авторизованного изображения 410b лица. Таким образом, возможности по компьютерной обработке, требуемые для выполнения второго этапа аутентификации, существенно снижаются по сравнению с ситуацией, когда на этапе аутентификации требуется сравнение со всеми хранимыми изображениями лица, т.е. с изображениями, которые принадлежат всем авторизованным людям, которые содержат скорректированные черты лица. Кроме того, поскольку центральный контроллер 145 выполнен с возможностью осуществления второго этапа аутентификации таким образом, что при аутентификации не требуется сравнение со всеми хранимыми изображениями, маловероятно, что произойдет сбой системы безопасности из-за невозможности принять правильное решение в отношении аутентификации людей с похожими чертами лица. В то же время злоумышленники, незаконно завладевшие первым маркером аутентификации, не смогут получить доступ, поскольку они не пройдут второй этап аутентификации, поскольку у них не будет изображений авторизованного человека с различными скорректированными чертами лица, которые соответствуют выбранным командам по коррекции лица, которые должны выполняться для получения определенных скорректированных черт лица для захвата изображения. Аналогичным образом, злоумышленники, которые могут предоставить только одно изображение лица должным образом авторизованного человека на фотографии, не пройдут второй этап аутентификации.

В некоторых вариантах осуществления маркер аутентификации может обеспечивать предоставление постоянного доступа в рабочее пространство 115. В других вариантах осуществления маркер аутентификации может обеспечивать предоставление временного доступа в рабочее пространство 115, например, на определенную конкретную неделю или доступ только в дневное время. В этом отношении центральный контроллер 145 может быть выполнен с возможностью предоставления доступа в рабочее пространство 115 только в том случае, если первый и/или второй этапы аутентификации выполняются человеком, пытающимся получить доступ в рабочее пространство 115 в допустимое, предварительно одобренное выбранное время. И наоборот, если человек пытается получить доступ в рабочее пространство 115 в любое время, отличное от допустимого, предварительно одобренного выбранного времени, доступ запрещается. Соответственно, при выполнении первого или второго этапа аутентификации текущее время осуществления доступа человеком может быть сравнено с предварительно одобренным выбранным временем, данные о котором хранятся для этого конкретного человека и связаны со штрих-кодом для этого человека. Предварительно одобренное время может быть введено для рабочего 105a и 105b для его сохранения в хранилище 114 данных компонента-запоминающего устройства центрального контроллера 145 посредством устройства 140 ввода, которым управляет, например, оператор-администратор системы 100 безопасности. Таким образом, в качестве примера, если для рабочего 105a авторизован доступ в рабочее пространство 115 днем, но не ночью, в то время как для рабочего 105b авторизован доступ в рабочее пространство 115 в любое время, при инициировании каждым из рабочих 105a и 105b процесса аутентификации, например, в 23:00 система 100 безопасности может отказать рабочему 105a в доступе в рабочее пространство 115, при этом предоставляя доступ рабочему 105b. Таким образом, система 100 безопасности может быть выполнена с возможностью управления доступом в рабочее пространство 115 по времени.

Как показано на фиг. 2, по меньшей мере в одном варианте осуществления модуль 109 аутентификации может содержать устройство 240 для измерения температуры, соединенное с центральным контроллером 145. Устройство 240 для измерения температуры установлено и выполнено с возможностью измерения температуры тела человека 410, находящегося в пространстве 117b для представления. Устройство 240 для измерения температуры может представлять собой устройство для измерения температуры, для которого требуется физический контакт между включенным в него датчиком температуры и человеком 410 в пространстве 117b для представления, например, путем обеспечения физического контакта между пальцем 410 человека и датчиком 241 температуры. Команды по коррекции лица человеку 410 для установления такого контакта могут быть выданы посредством устройства 210 для выдачи команд. Однако более предпочтительно устройство 240 для измерения температуры представляет собой устройство измерения температуры, включающее в себя датчик 241 температуры, который позволяет удаленно определять температуру, т.е. датчик температуры, для которого не требуется физический контакт между человеком 410 и датчиком 241 температуры, такой как, например, инфракрасное устройство для сканирования температуры, которое может работать на расстоянии в несколько дюймов от лба человека 410 или от других зон измерения.

Кроме того, в некоторых вариантах осуществления устройство 240 для измерения температуры может быть размещено и установлено с фиксацией на месте для обеспечения измерения температуры человека 410, находящегося в пределах пространства 117b для представления, например, путем неподвижного закрепления на опорных конструкциях 216a или 216b ворот. В других вариантах осуществления устройство 240 для измерения температуры может представлять собой портативное устройство, в том числе

переносное устройство, которым может управлять другой человек, когда человек 410 находится в пространстве 117b для представления.

Устройство 240 для измерения температуры может включать любой сканер температуры, термометр тела или другое устройство для измерения температуры тела человека, включая любой сканер температуры по времени, т. е. сканер температуры, более или менее непрерывно определяющий температуру тела в зависимости от времени. Устройства 240 для измерения температуры, которые могут использоваться в соответствии с настоящим документом, включают устройства для измерения температуры, описанные, например, в патенте США № 8282274.

В целом, устройство 240 для измерения температуры быть собой выполнено с возможностью измерения температуры тела человека 410 в пределах пространства 117b для представления, а затем передачи данных об измеренной температуре тела в центральный контроллер 145. Центральный контроллер 145 может быть выполнен с возможностью передачи сигнала на отпирание электронного замка 230, таким образом, разрешая открытие ворот 215 и позволяя человеку 410 получить доступ в рабочее пространство 115, если измеренная температура тела не отклоняется от температуры тела здорового человека, например, если температура тела не превышает допустимую заранее заданную температуру тела около 37, 37,5, 38 или 38,5°C. И наоборот, если измеренная температура тела отклоняется от температуры тела здорового человека и, например, превышает допустимую заранее заданную температуру тела, равную приблизительно 37, 37,5, 38 или 38,5°C, центральный контроллер 145 выполнен с возможностью не передавать сигнал на электронный замок 230, так что он может оставаться заблокированным, даже если рабочий прошел другие проверки безопасности. Таким образом, можно ограничить доступ в рабочее пространство 115 для людей, которые имеют, например, повышенную температуру тела, и допускать в рабочее пространство только людей 115, температура тела которых находится в предварительно определенном диапазоне температуры тела от приблизительно 36,5°C до приблизительно 38,5°C. Кроме того, центральный контроллер 145 может быть выполнен с возможностью уведомления человека 410, находящегося в пространстве 117b для представления, об измеренной температуре тела через устройство 210 для выдачи команд. В том случае, если человеку отказано в доступе в рабочее пространство 115 в результате обнаруженного отклонения от нормальной температуры тела, человек по желанию может пройти дополнительное отдельное медицинское обследование. Таким образом, этот пример осуществления может быть реализован для контроля распространения заразных заболеваний, которые вызывают повышение температуры тела человека 410 до значений, которые находятся за пределами заданного диапазона температуры тела.

Следует отметить, что в некоторых вариантах осуществления устройство 240 для измерения температуры может быть выполнено с возможностью работы в условиях, в которых могут происходить существенные колебания температуры окружающей среды, например, из-за изменения погодных условий. В этом отношении устройство 240 для измерения температуры может быть выполнено с возможностью учета изменений температуры окружающей среды. Например, в том случае, если человек 410 пытается получить доступ при низких зимних температурах, устройство 240 для измерения температуры вместе (в соответствующих случаях) с центральным контроллером 145 может быть выполнено с возможностью коррекции измеренной температуры тела в сторону повышения. Аналогичным образом, если человек 410 пытается получить доступ при высоких летних температурах устройство 240 для измерения температуры вместе (в соответствующих случаях) с центральным контроллером 145 может быть выполнено с возможностью коррекции измеренной температуры тела в сторону понижения. Вышеупомянутая коррекция, в частности, предпочтительна, когда устройство для измерения температуры измеряет температуру на поверхности кожи.

Следует отметить, что центральный контроллер 145 может быть выполнен с возможностью обеспечения того, чтобы устройство 240 для измерения температуры могло определять температуру тела человека 410 до выполнения этапа аутентификации, или во время выполнения первого и/или второго этапа аутентификации, или после выполнения второго этапа аутентификации.

В некоторых вариантах осуществления устройство 240 для измерения температуры также может представлять собой инфракрасный датчик, выполненный с возможностью определения теплового профиля на основании тепловых контуров человека 410 в пространстве 117b для представления. В таких вариантах осуществления центральный контроллер 145 может быть выполнен с возможностью передачи сигнала для отпирания электронного замка 230, таким образом, разрешая открыть ворота 215 и позволяя человеку получить доступ в рабочее пространство 115, только в том случае, если определенный тепловой профиль соответствует определенным характеристикам или атрибутам реального человека, находящегося в пространстве 117b для представления. Таким образом, например, центральный контроллер 145 может быть выполнен таким образом, что если человек 410 пытается обойти аутентификацию, представляя неодушевленный предмет, такой как изображение, на этапе аутентификации, на котором требуется представление черт лица человека 410, при обнаружении устройством 240 для измерения температуры теплового профиля, который не соответствует живому человеку 410, центральный контроллер 145 не разблокирует электронный замок 230

Следует отметить, что в представленных в настоящем документе вариантах осуществления, в кото-

рых устройство, принимающее первый маркер аутентификации, и камера, захватывающая изображение лица, разделены, эти устройства могут быть установлены на расстоянии друг от друга и даже могут быть расположены в разных пространствах (т.е. в разных местах). Таким образом, первый этап аутентификации может выполняться в первом пространстве, а второй этап аутентификации может выполняться во втором пространстве, например, в первом помещении и втором помещении. Доступом из первого пространства во второе пространство может управлять другое устройство управления доступом, предоставляющее доступ по завершении первого этапа аутентификации. На фиг. 6 показаны пространства 600a и 600b, которые отделены от наружного пространства 625 и отделены друг от друга стенкой 615. Чтобы человек мог получить доступ в пространство 600b, содержащее вычислительное устройство 106, выполняется первый этап аутентификации с использованием устройства 610 аутентификации, когда человек находится в наружном пространстве 625. После успешного завершения первого этапа аутентификации электронные ворота 630 разблокируются электронным устройством 605 управления доступом и человек может перейти из наружного пространства 625 в пространство 600a. Для получения доступа в пространство 600b выполняется второй этап аутентификации, причем каждый из первого и второго этапов аутентификации выполняется, как описано выше. Следует отметить, что, таким образом, человек, прошедший первый этап аутентификации, но не прошедший второй этап аутентификации, может находиться в пространстве 600a для дальнейшей проверки.

Еще в одном аспекте настоящего изобретения предложен по меньшей мере один вариант осуществления реализуемого на компьютере способа разблокировки электронного устройства управления доступом системы безопасности, включающего:

захват с помощью камеры первого изображения лица человека, находящегося перед камерой, при этом камера расположена рядом с электронным устройством управления доступом;

выполнение первого этапа аутентификации в двухэтапном процессе аутентификации человека, причем первый этап аутентификации включает:

прием первого маркера аутентификации от человека; и

аутентификацию человека с использованием первого маркера аутентификации; выполнение второго этапа аутентификации в двухэтапном процессе аутентификации человека, причем второй этап аутентификации включает:

выбор одной из множества команд по коррекции лица для указания человеку скорректировать по меньшей мере одну черту лица при формировании изображения камерой;

инициирование передачи устройством для выдачи команд выбранной команды по коррекции лица человеку;

захват с помощью камеры второго изображения лица человека, корректирующего по меньшей мере одну черту лица в соответствии с переданной командой по коррекции лица;

прием по меньшей мере части второго изображения лица, содержащего скорректированную черту лица; и

аутентификацию человека, если часть второго изображения лица совпадает с соответствующим хранимым авторизованным изображением человека из хранилища данных скорректированных изображений лица; и

разблокирование устройства управления доступом при успешной аутентификации человека на первом и втором этапах аутентификации.

Следует отметить, что этот способ включает прием по меньшей мере части второго изображения лица, поскольку в зависимости от фактической команды по коррекции лица для коррекции черты лица может потребоваться только часть изображения для захвата этой скорректированной черты лица, например, верхний левый квадрант лица человека, когда ему, например, указано закрыть глаз. В таком случае для аутентификации может потребоваться сравнение лишь части второго изображения лица, которое было захвачено, с соответствующим хранимым авторизованным изображением человека из хранилища данных скорректированных изображений лица, причем соответствующее хранимое авторизованное изображение лица должно включать в себя ту же часть изображения лица. Это может позволить ускорить обработку данных и аутентификацию человека для доступа в рабочее пространство.

По меньшей мере в одном варианте осуществления настоящего изобретения предложен способ, показанный на фиг. 5. Таким образом, настоящее изобретение включает в себя представленный на фиг. 5 способ 500 разблокировки электронного устройства управления доступом системы безопасности, управляющей доступом в охраняемое пространство, причем способ 500 включает первый этап 505, на котором человек предстает перед электронным устройством управления доступом, чтобы попытаться получить доступ к охраняемое пространство. Следует отметить, что возможен альтернативный вариант осуществления, в котором может проверяться температура человека, пытающегося получить доступ посредством электронного устройства управления доступом, как описано выше, для разблокирования электронного устройства управления доступом.

Способ 500 также содержит второй этап 510, который может быть инициирован автоматически или инициирован человеком, предпринимающим действие по запросу доступа в защищенное пространство, например, путем нажатия установленной кнопки или с помощью установленного телефона, либо мо-

бильного телефона, для инициирования выполнения способа 500. При инициировании способа 500 человек становится в непосредственной близости от электронного устройства управления доступом. Электронное устройство управления доступом может включать в себя ворота, которые обычно находятся в заблокированном положении при инициировании способа 500.

Способ 500 также включает третий этап 515, включающий захват первого маркера аутентификации, например, штрих-кода или биометрических признаков, таких как полное или частичное изображение лица человека, который пытается получить доступ. Этот захват выполняется с помощью камеры. Камеру устанавливают в непосредственной близости от зоны представления, в которую становится человек, и расположенную, как правило, в непосредственной близости от ворот.

Способ 500 также включает четвертый этап 520, включающий аутентификацию человека на первом этапе аутентификации с использованием центрального контроллера. Этот этап выполняется путем сравнения первого маркера аутентификации с хранимыми авторизованными маркерами аутентификации, например, путем сравнения захваченного изображения лица с хранимыми авторизованными изображениями лица человека, хранимыми в хранилище данных. В том случае, если соответствующее изображение лица не идентифицировано, выполняется пятый этап 525, на котором человеку отказывают в доступе, например, при этом не открываются заблокированные ворота.

В том случае, если человек успешно аутентифицирован на первом этапе аутентификации, центральный контроллер выполняет шестой этап 530 способа 500. Шестой этап 530 включает выбор команды по коррекции черты лица из множества команд по коррекции черты лица. Выбранная команда по коррекции лица передается человеку с помощью устройства 210 для выдачи команд, как указано на седьмом этапе 535. Человек реагирует в соответствии с выбранной командой по коррекции лица, корректируя по меньшей мере одну из своих черт лица, в то время как камера захватывает изображение лица человека с по меньшей мере одной скорректированной чертой лица.

Способ 500 также включает восьмой этап 540, включающий повторную аутентификацию человека с использованием центрального контроллера. Этот этап выполняется путем сравнения захваченного скорректированного изображения лица с хранимыми авторизованными скорректированными изображениями лица человека, хранимыми в хранилище данных. В том случае, если соответствующее хранимое авторизованное скорректированное изображение лица не идентифицировано, выполняется пятый этап 525, на котором человеку отказывают в доступе, например, при этом не открываются заблокированные ворота. В том случае, если хранимое авторизованное скорректированное изображение лица идентифицировано как соответствующее захваченному скорректированному изображению лица, выполняется девятый этап 545 способа 500 и электронное устройство защиты доступа предоставляет человеку доступ в защищенное пространство, например, путем отпирания ворот. Затем, когда другой человек подойдет к электронному устройству управления доступом, выполнение способа 500 может быть повторено.

Следует отметить, что, хотя различные функции были описаны как выполняемые центральным контроллером, по меньшей мере в одном варианте осуществления эти функции могут выполняться другим вычислительным устройством, которое может быть локальным по отношению к электронным воротам.

Хотя идеи заявителя, описанные в настоящем документе, в иллюстративных целях представлены в виде различных вариантов реализации или вариантов осуществления, предполагается, что эти идеи заявителя не ограничиваются такими вариантами реализации. Напротив, идеи заявителя, описанные и проиллюстрированные в настоящем документе, охватывают различные альтернативы, изменения и эквиваленты, не выходящие за рамки описанных в настоящем документе вариантов реализации или вариантов осуществления, общий объем которых определяется прилагаемой формулой изобретения.

ФОРМУЛА ИЗОБРЕТЕНИЯ

1. Система безопасности, содержащая:

устройство управления доступом с электронной блокировкой, выполненное с возможностью разблокировки при аутентификации человека, находящегося перед устройством управления доступом; и

модуль аутентификации, соединенный с устройством управления доступом и содержащий:

устройство для выдачи команд;

камеру, выполненную с возможностью захвата первого изображения лица, по меньшей мере части лица человека, находящегося перед камерой; и

центральный контроллер, содержащий процессор и запоминающее устройство, выполненное с возможностью осуществления к нему доступа процессором, причем центральный контроллер соединен с возможностью обмена данными с устройством для выдачи команд и камерой, а запоминающее устройство содержит хранящиеся в нем программные команды, которые при их исполнении процессором конфигурируют центральный контроллер для выполнения первого этапа аутентификации в двухэтапном процессе аутентификации человека, причем первый этап аутентификации включает прием первого маркера аутентификации от человека и аутентификацию первого маркера аутентификации; и выполнения второго этапа аутентификации в двухэтапном процессе аутентификации человека, причем второй этап аутентификации включает:

выбор одной из множества команд по коррекции лица для указания человеку скорректировать по меньшей мере одну черту лица при формировании изображения камерой;

отправку выбранной команды по коррекции лица на устройство для выдачи команд;

выдачу выбранной команды по коррекции лица через устройство для выдачи команд человеку;

захват посредством камеры второго изображения лица человека, в то время как человек корректирует по меньшей мере одну черту лица в соответствии с переданной командой по коррекции лица;

прием центральным контроллером по меньшей мере части второго изображения лица, содержащего по меньшей мере одну скорректированную черту лица человека; и

аутентификацию человека, если часть второго изображения лица совпадает с соответствующим хранимым авторизованным скорректированным изображением лица человека, полученным из хранилища данных скорректированных изображений лица человека; и

разблокирования устройства управления доступом при успешной аутентификации на первом и втором этапах аутентификации.

2. Система безопасности по п.1, в которой второй этап аутентификации выполняется только при успешной аутентификации на первом этапе.

3. Система безопасности по п.1 или 2, в которой камера выполнена с возможностью захвата и приема первого маркера аутентификации.

4. Система безопасности по любому из пп.1-3, в которой модуль аутентификации содержит дополнительное устройство, которое выполнено с возможностью приема первого маркера аутентификации и которое представляет собой устройство, отличное от камеры.

5. Система безопасности по любому из пп.1-4, в которой центральный контроллер связан с возможностью обмена данными с хранилищем данных, содержащим множество сохраненных авторизованных маркеров аутентификации, а первый этап аутентификации включает выполнение сопоставления между принятым маркером аутентификации и хранимыми авторизованными маркерами аутентификации, причем каждый хранимый авторизованный маркер аутентификации связан с хранимыми авторизованными изображениями лица, содержащими скорректированные черты лица человека, а центральный контроллер выполнен с возможностью осуществления аутентификации на втором этапе аутентификации путем выполнения сопоставления исключительно между захваченным скорректированным изображением лица и одним из хранимых авторизованных изображений лица, которые связаны с первым маркером аутентификации и содержат указанные скорректированные черты лица человека.

6. Система безопасности по п.5, в которой по меньшей мере одно из хранимых авторизованных изображений лица, которое соответствует захваченному скорректированному изображению черты лица, имеет одну или более коррекций лица, которая соответствует одной или более коррекциям лица, заданным в предоставленной команде по коррекции лица.

7. Система безопасности по любому из пп.1-6, в которой первый маркер аутентификации содержит 1D или 2D штрих-код.

8. Система безопасности по любому из пп.1-6, в которой первый маркер аутентификации содержит первое изображение лица, захваченное камерой, а аутентификация включает выполнение сопоставления между захваченным первым изображением лица и хранилищем данных, содержащим хранимые в нем авторизованные изображения лица.

9. Система безопасности по любому из пп.1-8, в которой камера или устройство для выдачи команды расположены в непосредственной близости от устройства управления доступом с электронной блокировкой.

10. Система безопасности по любому из пп.1-9, в которой устройство для выдачи команд выполнено с возможностью выдачи визуальных команд или звуковых команд человеку, при этом визуальные команды при необходимости включают в себя анимацию, представляющую скорректированную черту лица, или текстовые команды для человека по коррекции по меньшей мере одной из его черт лица.

11. Система безопасности по любому из пп.1-10, в которой центральный контроллер выполнен с возможностью выполнения первого и второго этапов аутентификации в разных, соответственно первом и втором, пространствах.

12. Система безопасности по п.11, в которой электронное устройство управления доступом содержит первый и второй электронные компоненты управления доступом, причем первый электронный компонент управления доступом разблокируется после успешной аутентификации на первом этапе аутентификации, а второй электронный компонент управления доступом разблокируется после успешной аутентификации на втором этапе аутентификации.

13. Система безопасности по любому из пп.1-12, в которой центральный контроллер выполнен с возможностью разблокирования устройства управления доступом только в том случае, если первый и/или второй этапы авторизации также выполнены в выбранное предварительно одобренное время.

14. Система безопасности по любому из пп.1-13, в которой электронное устройство управления доступом также включает в себя устройство для измерения температуры, выполненное с возможностью измерения температуры тела человека, причем устройство для измерения температуры соединено с центральным контроллером, а центральный контроллер выполнен с возможностью разблокирования устрой-

ства управления доступом, если измеренная температура тела человека находится в заданном диапазоне температуры тела, при этом предпочтительно устройство для измерения температуры выполнено с возможностью измерения температуры тела человека после выполнения первого и второго этапов аутентификации, и при необходимости заданная температура тела находится в диапазоне от приблизительно 36,5 до приблизительно 38,5°C.

15. Реализуемый на компьютере способ разблокировки электронного устройства управления доступом системы безопасности, включающий:

захват с помощью камеры первого изображения лица человека, находящегося перед камерой, при этом камера расположена рядом с электронным устройством управления доступом;

выполнение первого этапа аутентификации в двухэтапном процессе аутентификации человека, причем первый этап аутентификации включает прием первого маркера аутентификации от человека и аутентификацию человека с использованием первого маркера аутентификации;

выполнение второго этапа аутентификации в двухэтапном процессе аутентификации человека, причем второй этап аутентификации включает:

выбор одной из множества команд по коррекции лица для указания человеку скорректировать по меньшей мере одну черту лица при формировании изображения камерой;

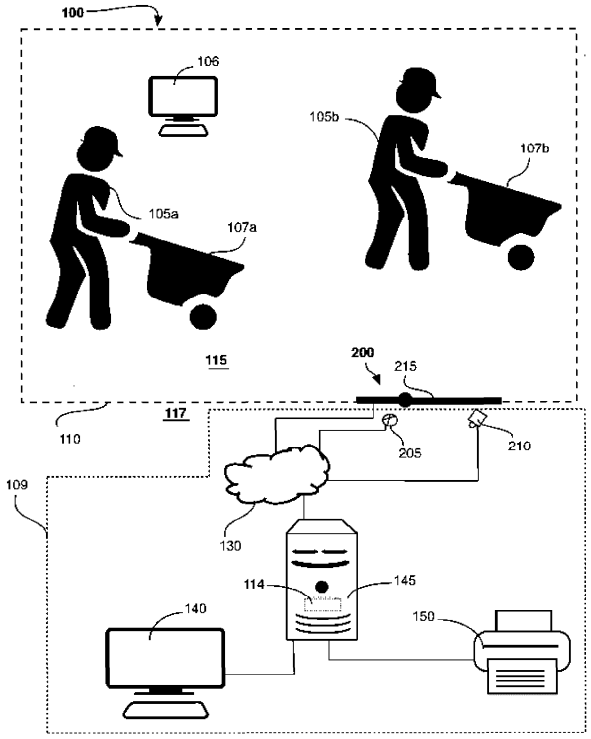
инициирование выдачи устройством для выдачи команд выбранной команды по коррекции лица человеку;

захват посредством камеры второго изображения лица человека, корректирующего по меньшей мере одну черту лица в соответствии с выданной командой по коррекции лица;

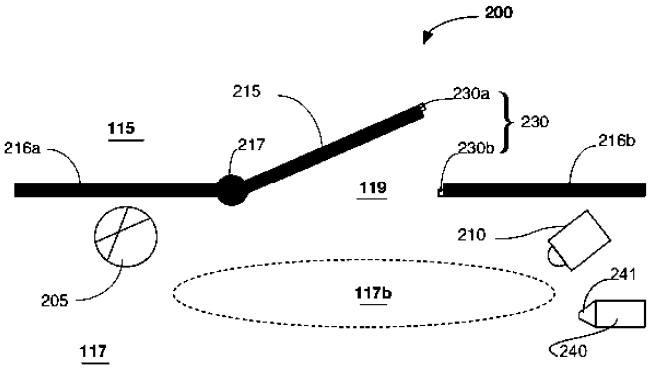
прием по меньшей мере части второго изображения лица, содержащего скорректированную черту лица; и

аутентификацию человека, если часть второго изображения лица совпадает с соответствующей частью хранимого авторизованного изображения человека из хранилища данных хранимых авторизованных скорректированных изображений лица; и

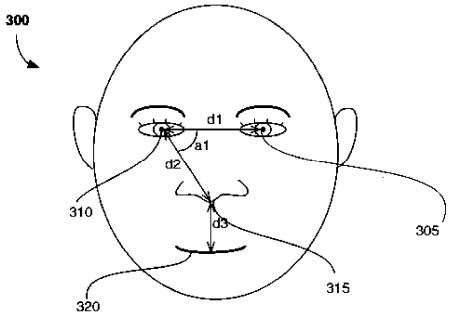
разблокирование устройства управления доступом при успешной аутентификации человека на первом и втором этапах аутентификации.



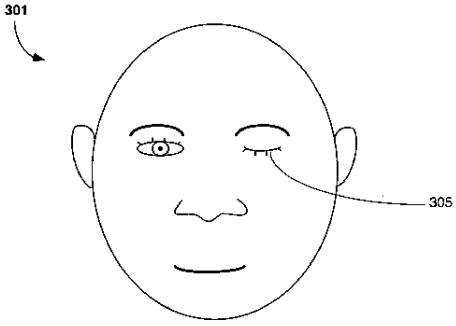
Фиг. 1



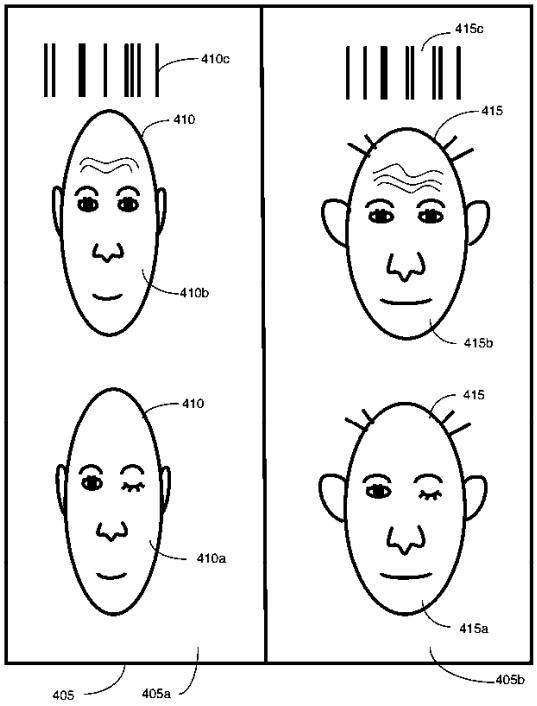
Фиг. 2



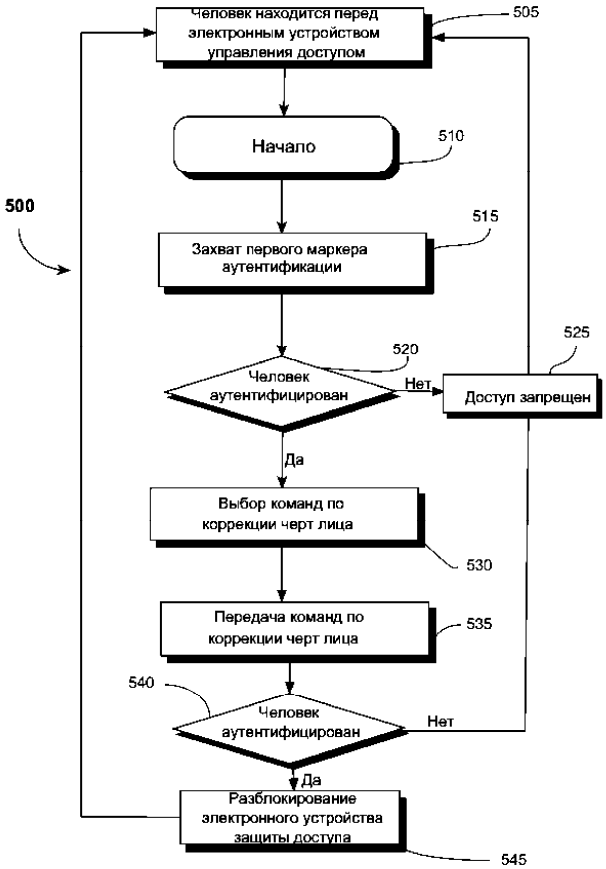
Фиг. 3A



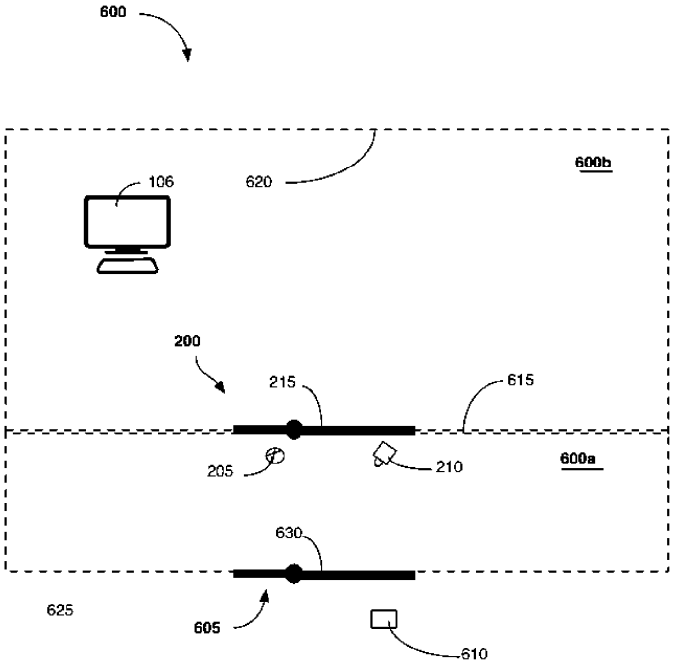
Фиг. 3B


410c
410
410b
410
410a
405
405a
415c
415
415b
415
415a
405b

Фиг. 4


500
Человек находится перед электронным устройством управления доступом
505
Начало
510
Захват первого маркера аутентификации
515
Человек аутентифицирован
520
Нет
Доступ запрещен
525
Да
Выбор команд по коррекции черт лица
530
Передача команд по коррекции черт лица
535
Человек аутентифицирован
540
Нет
Да
Разблокирование электронного устройства защиты доступа
545

Фиг. 5



Фиг. 6