CLAIMS

1. An access control method, comprising:

performing, by a camera device, video data collection to obtain video data;

performing, by the camera device, face image detection on the video data;

in response to a face image being detected, performing, by the camera device, authentication on the face image; and

outputting, by the camera device according to a result of the authentication, a corresponding access control signal, the access control signal being used for opening or closing a door by an access control linkage apparatus.

2. The method according to claim 1, wherein the performing, by the camera device, face image detection on the video data comprises: selecting, by the camera device, an image from the video data, and performing face detection on the selected image based on a deep learning network;

a face image being detected comprises: a face being detected in the selected image; and

the performing, by the camera device, authentication on the face image comprises：performing, by the camera device, feature data extraction on the face image based on the deep learning network，and performing authentication on the extracted feature data based on a feature database built in the camera device.

3. The method according to claim 2, wherein the outputting, by the camera device according to a result of the authentication, a corresponding access control signal comprises:

if the extracted feature data passes the authentication, outputting, by the camera device, a door opening control signal, the door opening control signal being used for performing a door opening operation by the access control linkage apparatus.

4. The method according to claim 3, wherein after the outputting, by the camera device, a door opening control signal, the method further comprises:

in response to no face image being detected within a preset time period, outputting, by the camera device, a door closing control signal, the door closing control signal being used for performing a door closing operation by the access control linkage apparatus.

5. The method according to any one of claims 2 to 4, wherein the feature database comprises a whitelist, the whitelist is used for storing first user information, and the first user information comprises: face feature data of a user permitted to pass;

the performing authentication on the extracted feature data based on a feature database built in the camera device comprises:

identifying whether face feature data consistent with the extracted feature data exists in the whitelist; and

if the face feature data consistent with the extracted feature data exists in the whitelist, the extracted feature data passes the authentication; if no face feature data consistent with the extracted feature data exists in the whitelist, the extracted feature data does not pass the authentication.

6. The method according to claim 5, further comprising:

if no face feature data consistent with the extracted feature data exists in the whitelist, outputting, by the camera device, prompt information indicating that the current user is a stranger.

7. The method according to any one of claims 2 to 6, wherein the feature database comprises a blacklist, the blacklist is used for storing second user information, and the second user information comprises: face feature data of a user forbidden to pass;

the performing authentication on the extracted feature data based on a feature database built in the camera device comprises:

identifying whether face feature data consistent with the extracted feature data exists in the blacklist; and

if the face feature data consistent with the extracted feature data exists in the blacklist, the extracted feature data does not pass the authentication.

8. The method according to any one of claims 5 to 7, wherein a fact that the face feature data consistent with the extracted feature data exists comprises:

a fact that face feature data having similarity of greater than a preset threshold to

the extracted feature data exists.

9. The method according to any one of claims 1 to 8, wherein the outputting, by the camera device according to whether the extracted feature data passes the authentication, a corresponding access control signal comprises:

if the extracted feature data does not pass the authentication and an electronic door in the access control linkage apparatus is currently in an open state, outputting, by the camera device, a door closing control signal, the door closing control signal being used for performing a door closing operation by the access control linkage apparatus.

10. The method according to any one of claims 6 to 9, further comprising:

if the face feature data consistent with the extracted feature data exists in the blacklist, controlling, by the camera device, an alarm apparatus to give an alarm.

11. The method according to any one of claims 2 to 10, further comprising:

collecting an image;

performing face detection on the collected image;

in response to a face being detected in the collected image, extracting feature data of the face in the collected image to obtain the face feature data of the user permitted to pass; and

establishing, based on the face feature data of the user permitted to pass, corresponding first user information in the feature database, the first user information comprising: the face feature data of the user permitted to pass.

12. The method according to claim 11, wherein the establishing, based on the face feature data of the user permitted to pass, corresponding first user information in the feature database comprises:

sending the face feature data of the user permitted to pass and corresponding user identification information to the camera device by means of a terminal device; and

establishing, by the camera device, the first user information of the user permitted to pass in the whitelist of the feature database, the first user information further comprising the user identification information corresponding to the face feature data.

13. The method according to any one of claims 2 to 12, further comprising:

sending the second user information of the user forbidden to pass to the camera device by means of the terminal device, the second user information comprising: the face feature data of the user forbidden to pass; and

storing, by the camera device, the second user information of the user forbidden to pass in the blacklist of the feature database.

14. The method according to claim 13, wherein the second user information further comprises user identification information of the user forbidden to pass.

15. The method according to any one of claims 1 to 14, further comprising:

recording, by the camera device, user passage information in a monitoring log, the user passage information comprising information of each user and a time when the user passes through the access control linkage apparatus or fails to pass the authentication.

16. The method according to claim 15, further comprising:

in response to reception of a query request, querying the user passage information satisfying a query condition in the query request from the monitoring log and outputting said information.

17. An access control apparatus, comprising:

a first collection module, configured to perform video data collection to obtain video data;

a first face detection module, configured to perform face image detection on the video data, and in response to a face image being detected, perform authentication on the face image; and

a control module, configured to output, according to a result of the authentication output by the first face detection module, a corresponding access control signal, the access control signal being used for opening or closing a door by an access control linkage apparatus.

18. The apparatus according to claim 17, wherein the first collection module is further configured to select an image from the video data to send to the first face detection module; and

the first face detection module is configured to: perform face detection on the selected image based on a deep learning network; and in response to a face being detected in the selected image, perform feature data extraction on the face image based on the deep learning network, and perform authentication on the extracted feature data based on a feature database.

19. An access control system, comprising:

a terminal device, configured to: collect an image; perform face detection on the collected image; and in response to a face being detected in the collected image, perform feature data extraction on the face in the image to obtain face feature data of a user permitted to pass, and send the face feature data to a camera device; and

a camera device, configured to: receive the face feature data of the user permitted to pass sent by the terminal device, and store the face feature data of the user permitted to pass in a feature database built in the camera device; perform video data collection to obtain video data; perform face image detection on the video data; in response to a face image being detected, perform feature data extraction on the face image, and perform authentication on the extracted feature data based on the feature database; and output, according to a result of the authentication, a corresponding access control signal, the access control signal being used for opening or closing a door by an access control linkage apparatus.

20. A computer-readable medium, configured to store computer-readable instructions, wherein when the instructions are executed, operations of the operations in the access control method according to any one of claims 1 to 16 are implemented.