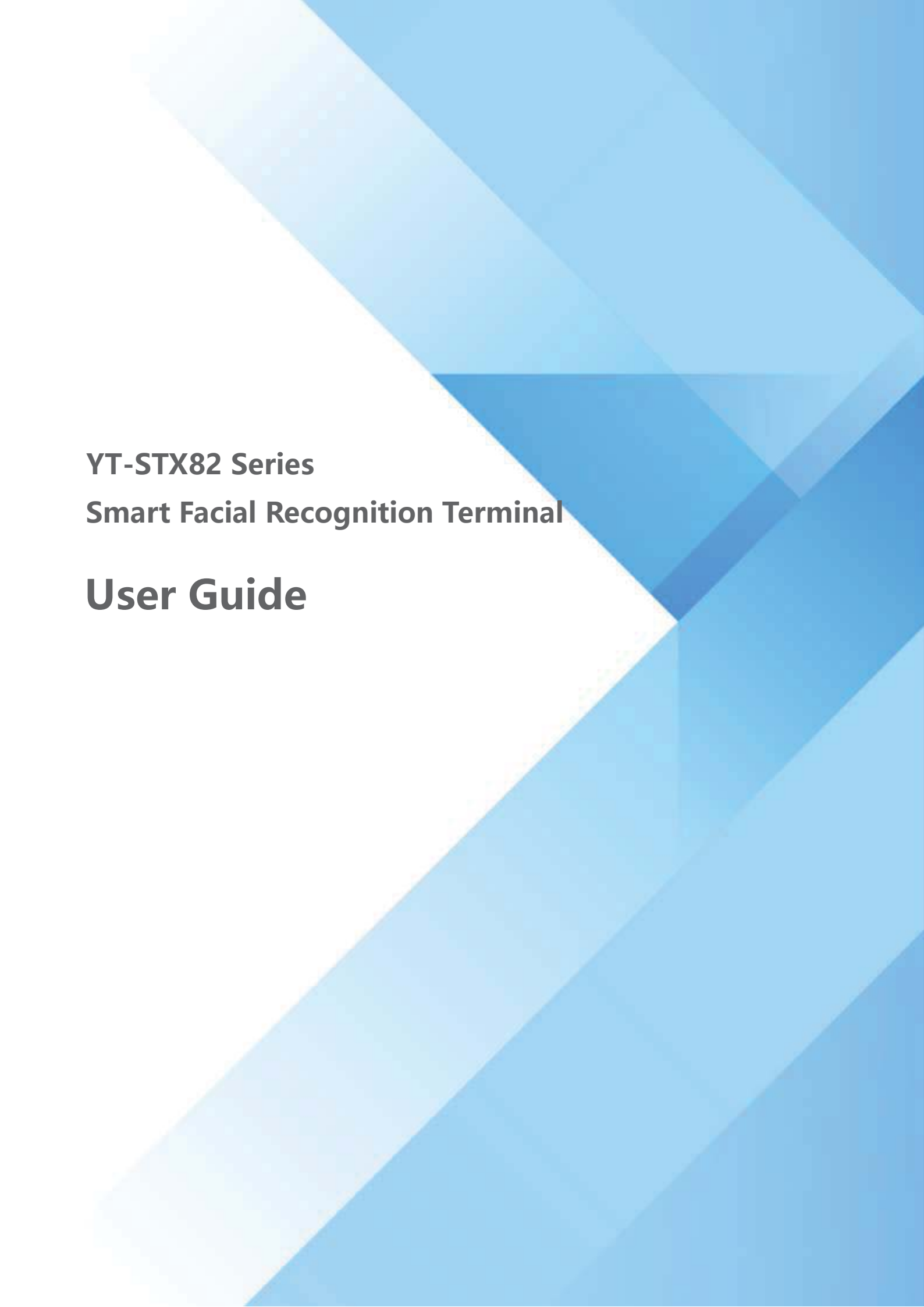




YT-STX82 Series

Smart Facial Recognition Terminal

User Guide

Content

1	Preface	6
1.1	General	6
1.2	Operation Notice	6
1.3	Marks Usage Agreement	6
2	Introduction.....	8
2.1	Main parts	8
2.2	Interfaces.....	9
2.3	Specifications.....	10
3	Operational Environment.....	12
3.1	Environmental requirements.....	12
3.2	Installation requirements.....	12
3.3	Lens.....	13
4	Operations	14
4.1	Login.....	14
4.2	System Settings	15
4.2.1	Device Info.....	16
4.2.2	Face management.....	17
4.2.3	Access control.....	18
4.2.4	Hardware setup.....	21
4.2.5	Network settings.....	23
4.2.6	Surveillance information.....	24
4.2.7	Verification settings.....	25
4.2.8	Human body temperature measurement settings	26
4.2.9	About.....	26
5	platform to access.....	27
5.1	Active connection.....	27
5.2	Passive access in the platform.....	30
	Appendix Proper Nouns.....	31

About This Manual

The Company can update this manual at any time without prior notice and any responsibility. If you need the latest version of the manual, please contact us.

This manual is used as a user manual. The photos, figures, charts, and illustrations, etc., are used to explain this manual only. This manual is just for reference, and actual products may be different from this manual.

Within the maximum scope permitted by law, the products described in this Manual (including hardware, software, firmware, etc.) are provided "**AS IS**". The information in this document (including URL and other Internet site reference data) is subject to change without notice. This Manual may contain technical inaccuracy or printing errors. This information will be periodically changed, and these changes will be incorporated into the latest version of this Manual.

Safety Precautions

CAUTION Failure to follow the safety instructions in this manual may result in fire, electric shock, or other injuries. It may also damage the product or other properties. Before using this product, please read all the safety notifications below.

Fair and Reasonable Usage In the process of using, the user should follow the technical parameters of the product and its accessories, pay conscious attention, fulfill protection obligations, and use the product in good faith. The Company does not undertake any free maintenance obligation for products that were damaged due to user's fault. Also, the user shall use this product by following the product manual and the training contents related to the user manual. Unless otherwise agreed, the user shall not sublease, resell, or transfer the product to others.

Operational Environment This product and its accessories should be used in the daily living environment. The whole product is not intended for use in extreme environments, such as temperatures below -20°C or above 55°C, or in a humid air environment. The server for this product needs to be stored in a physical environment such as the computer room, data center, and independent room to ensure stable operation of the product. Using a damaged cable or power line or using the product in a humid environment can result in fire, electric shock, injury, or damage to the product or other properties. Please do not expose the hardware to a high-temperature environment or heat-generating equipment such as sunlight, heaters, microwave ovens, ovens, or water heaters.

Maintenance This product does not contain any other parts that a user can repair. Please do not open or remove the hardware of this product or attempt to repair or replace any part of it. Removing the hardware may cause damage to the product or personal injury. If this product is damaged or malfunctioned, please contact us. If the user tries to open the product, it may cause damage to the product, and the warranty of this product will not cover the damage.

Electromagnetic Field The hardware equipment contained in this product may include components and wireless devices that generate magnetic fields and may interfere with heart pacemakers, defibrillators, or other medical devices. There should be a safe distance between the hardware and the user. Please consult your physician and medical device manufacturer for specific medical device information.

External Device This product and its accessories support third-party external devices that meet product specifications, such as cables, wires, and power supplies. Before using a third-party device, please ensure that the third-party device complies with relevant laws and regulations, the technical specifications of the product, and ensure that the usage complies with requirements of third-party devices and the product. Usage that does not comply with laws and regulations or national standards, or using power supplies, cables and other devices that are not recognized by the Company or incompatible with the product may cause the fire, explosion, or other dangers. The Company is not liable to provide free maintenance resulting from the use of external devices that do not meet the requirements of this manual. If you use unauthorized devices, you may void the warranty of the product and violate the relevant regulations of the country where the product is located and may cause a safety accident.

For more information regarding external devices, please contact us.

Battery If the product and its accessories are equipped with a non-removable internal battery, please do not replace the battery by yourself in case the battery or the product is damaged. The battery can only be replaced by the Company or Company authorized service providers. Please dispose of this product, batteries and other accessories in accordance with local regulations and do not dispose them as household waste. Improper handling of the battery can lead to heat generation, explosion or fire.

Use of The Product

Unless otherwise specified, the software of the product is for use only. Without the permission of the relevant copyright holder, no one may copy, distribute, modify, extract, decompile, disassemble, decrypt, reverse engineer, lease, transfer, resell, and otherwise infringe the copyright of the software in any form, except that such behaviors are permitted by law. In addition, the Company shall not be responsible for any liability due to software or hardware intellectual property infringement by any third parties, whose software or hardware is contained by this product.

No Endorsement The Company does not endorse the content generated by any user in the Company's products or any opinions, recommendations or suggestions expressed therein. The Company expressly stated that the Company is not liable for any responsibility in relation to the content produced in the software.

This product should not be used for illegal or prohibited purposes. The company does not allow anyone to use the Company's products to infringe the privacy, personal information, and portrait rights of others.

The user shall not use this product for any illegal use or any prohibited use under these

terms, conditions, and declarations. When using this product, the User shall not damage, disable, overload or obstruct any of the hardware of this product in any way, or interfere with the use of this product by any other users. Also, the user should not attempt to use the product or the software, by hacking, stealing the password, or any other means. Moreover, the user should not obtain or attempt to obtain any data or information not explicitly provided by the software through any means.

Disclaimer

As to any defects, errors, or failures that may exist, the Company does not provide any kind of express or implied warranties in all contents of this manual, including but not limited to the merchantability, quality satisfaction, fitness for specific purposes, no infringing third parties' rights, etc. The Company does not compensate any special, incidental, occasional and indirect damages resulting from the use of this manual or use of the Company's products, including but not limited to the loss of business profits, loss of data or loss of documentation.

If the user connects the product to the Internet, the person must take risks, including but not limited to the risk that may be subject to cyber-attacks, hacking, virus, etc. Within the scope permitted by laws, the Company is not liable to the responsibility for malfunctions and information leakages and so on, caused by the previous reasons, but the Company will provide prompt product-related technical support to the user.

When using this product, the user should strictly follow the applicable laws. If the product is used for infringing a third party's rights or other improper use, the Company shall not bear any liabilities.

If the content of this manual conflicts with applicable laws, the provisions of the law shall prevail.

Import and Export Controls

If products and its accessories described in this product manual (including but not limited to the software and technical data in the product) need to be exported, re-exported or imported, the user shall comply with applicable import and export control laws and regulations.

Privacy Protection

The Company respects all applicable laws, regulations, judicial interpretations, and other legal-binding documents regarding the protection of personal information and personal privacy protection. To protect personal information and privacy, the user is required to comply with these laws, regulations, decrees, and documents when using this product.

1 Preface

1.1 General

This manual is suitable for YT-STX82 series, the software version 5.0.x. This article guides you to understand and use this product.

Infrared thermal imaging module YT-STX82-APHG adapted to YT-STX82 series products. The module can be directly installed with YT-STX82 on site and can be used.

1.2 Operation Notice

- Please read through the Manual carefully prior to using the product. Save the Manual properly for further references. This Manual has been reviewed.
- Views in this Manual serves as a reference only.
- The guide will be updated at any time without prior notice.
- In case of any doubt or dispute of this user guide, the final explanations from our company shall prevail. We assume no responsibility for any consequences caused by the user misunderstands, improper operations.

1.3 Marks Usage Agreement

The following warning signs are used in this guide:

CAUTION



Indicate operations that may cause device damage or data loss.

Note



Indicate useful information that requires attention when operating.

The following editorial conventions are used in the guide:

Convention	Description
Bold	Field names / button names are written in bold
<i>Italic</i>	Commands, file names and paths are written in italic and bold
>	Indicate sequential mouse clicks on user interfaces.

2 Introduction

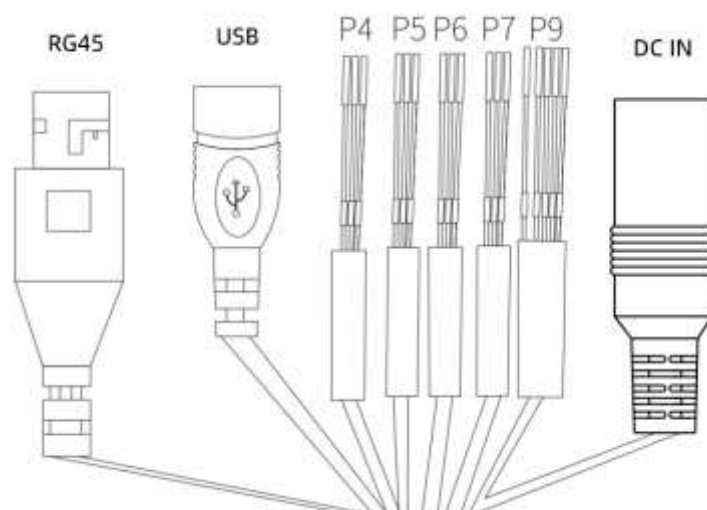
YT-STX82 series Smart Facial Recognition Terminal, powered by industry-leading deep learning face recognition algorithm, can be used with turnstiles or wall-mount indoors and outdoors and can bring better and safer access control.

With surveillance management platform, it can help you with better personnel management, device management and record management, and can be widely applied in the entrances and exits of office buildings, factories and campuses with a “zero-second” access experience.

2.1 Main parts

Number	Description
1	Infrared fill light
2	RGB camera
3	Infrared camera
4	White light fill light
5	Human body detection (infrared sensor module)
6	Multi-point capacitive touch screen
7	Card reader
8	Speaker
9	Microphone
10	Reset button
11	Fixing screw holes for accessories
12	Fixing screw holes for Wall mounting, or turnstiles

2.2 Interfaces



Interface Name	Description
USB	USB 2.0
RJ45	10/100 Mbps
Power	12V DC Input
P4	Relay (NC、COM、 NO)
P5	Wiegand (D1、 D0、 GND)
P6	RS485 (485A, 485B, GND)
P7	Serial port (GND、 TXD、 RXD)
P9	Dry contact & GPIO (RECOVER、 GPIO、 IN1、 IN2、 GND)

2.3 Specifications

Product Specifications	Parameter
Terminal dimensions	236 mm X 131mm X 20mm
Operating system	Android 7.1
CPU	64 bit 6-core CPU
Memory	2GB DDR3L
Flash memory	16GB eMMC
Camera	2M pixel visible light camera 2M pixel infrared camera
Screen	8-inch Multi-touch screen, Resolution 800*1280
Network connection	10/100 Mbps wired 2.4G WIFI
Interface	• Wiegand output *1 • Relay output *1 • Contact monitoring input *2 • USB 2.0 * 1 • RS485 * 1 • Serial port Uart * 1 • GPIO input * 1 • Recovery * 1
Audio	• Waterproof MIC • Waterproof speaker 1W x 2
Infrared fill light	Support
White light fill light	Support (self-adaptive)
Human body detection	Support (Infrared sensor module)
Card reader	IC card supported (ISO14443A)
Human body detection	Support
Liveness detection	Support
Facial recognition	Support
Infrared Thermal Imaging Module	YT-STX82-APHG
Temperature sensor	Vanadium oxide microbolometer
Resolution	120 x 90 @17μm WLP
Focal length	2.3mm F1.1
Field of view	50°±1°
Shutter scheme	Automatic built-in shutter

Accuracy	±0.5°C (16°C-32°C)
Range	20°C-50°Cd (28-42°C)
Distance	0.5m~1.2m
Data	120 x 90 14Bit @ 25FPS
Operational Environment	
Power Supply	AC 100 V – 240 V
Operating Voltage	DC 12 V $\Rightarrow$ 1.8 A
Heat dissipation	Passive cooling
Operating temperature	-10 °C - 60 °C(YT-STX82 use only) 0 °C~40 °C(YT-STX82 with YT-STX82-APHG)
Operating relative humidity	5%~95% (without condensation)
Protection level	IP66 (YT-STX82 use only) Indoor (YT-STX82 with YT-STX82-APHG)

3 Operational Environment

Cautions



All electrical regulations of the country and region must be strictly followed during the installation and use of this product. If the equipment is not working properly, please do not disassemble and repair it by yourself, otherwise it will affect the equipment warranty. During installation and use, it is necessary to avoid extreme or extreme environments such as extreme high temperature (or low temperature) , high humidity, high backlighting, vibration, radiation, and chemical corrosion.

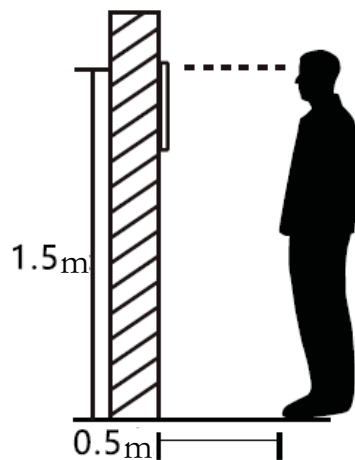
3.1 Environmental requirements

- Light environment: It is recommended to install indoor or semi-open air environment to ensure a good light environment, avoid direct light or weak light affecting the recognition speed, and avoid directly facing the glass door or glass wall. Network: It is recommended to install in an unobstructed network to avoid impact on recognition speed and accuracy.
-

3.2 Installation requirements

The recommended installation height (the height of cameras of YT-STX82) which can cover human height of 1.55m - 1.85m when the distance between the person and the panel is 0.5m.

It can be adjusted according to the effect of face image acquired by the device. When the face image is large, it can move backward properly; when the face image is small, it can move forward properly.



When using the device for registration and identification, the installation location of the device must remain unchanged. If you really need to move the device, you must keep the installation height consistent. If it is inconsistent, it may affect the recognition effect. It is recommended that the distance between the face and the machine at the time of registration is 0.5-0.8 meters.

Description



This product can be used for access control or gate channel installation. For specific installation methods, please refer to the Quick Installation Manual and Operation and Maintenance Manual.

3.3 Lens

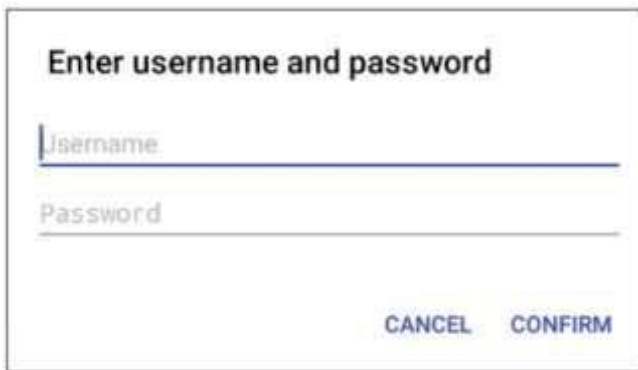
If you find the picture taken is unclear, please check if the camera lens is clean in the first place. Please clean the camera with a lens cleaning cloth. Do not touch the camera with fingers or rough objects, which may cause the damage on the camera lens.

4 Operations

4.1 Login

Follow these steps to log on the device:

1. Power on the device. When system initialization completes, the screen will show the working interface.



Description



The user needs to select system language (simplified Chinese / English) for the first login or after the device is restored to factory defaults.

2. Tap on the bottom-right of the screen , enter username and password and tap **CONFIRM** to log on the device.

There are two types of accounts: administrator and operator. The default username and password for the above two accounts are administrator/administrator, operator/operator. After login, administrators can create new accounts ((including administrator account)), delete other accounts or modify their rights in **Settings > Account management**.

Cautions



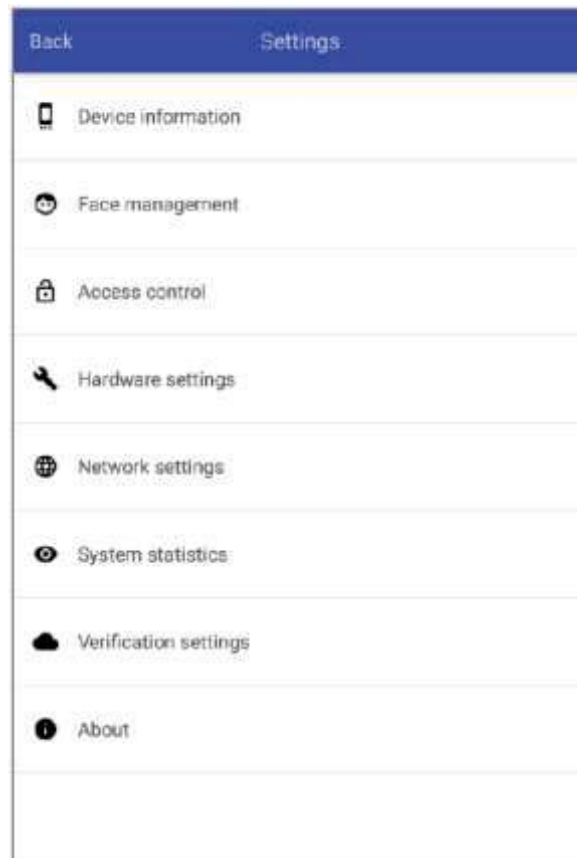
It is strongly recommended to change the default password after the first login (**Settings > Device information > Change password**). The new password must contain at least nine characters, which includes at least one numerical digit, one special character, and both lower and

uppercase alphabetical characters.

If the user continuously tries to log on the device with wrong username or pass- word more than 5 times, the CONFIRM button will be disabled for 3 minutes.

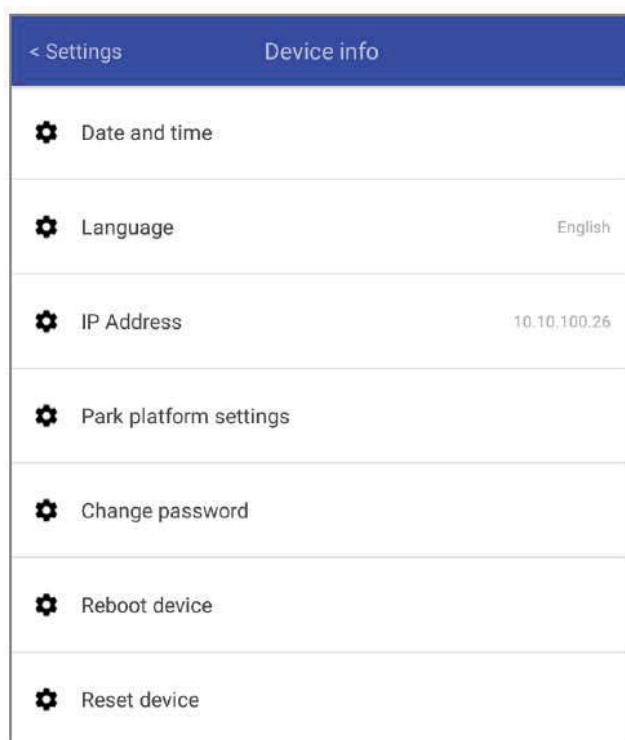
4.2 System Settings

After login, you can view device information, monitor statistics, software version and configure access mode, audio, network and comparison settings on **Settings** page. You can also manage face images locally when the device is not connected the management platform.



4.2.1 Device Info

Settings > Device information to view the information on the device.



Device name/location	Specify the device name and location to distinguish different devices.
Date and time	Set the time server and time zone to keep the system time and the network time in sync.
Language	Switch system languages (Simplified Chinese/English).
IP Address	The IP address of the current device.
Park platform settings	Connect the device to park platform on device side (active connection) . Refer to Connecting to park platform for details.
Change a password	Change login password. The password must contain at least nine characters, which includes at least one numerical digit, one special character, and both lower and uppercase alphabetical characters.
Reboot device	Restart the device.
Reset device	All data of the device will be cleared. Please operate with cautions.

4.2.2 Face management

Cautions



When the device is connected to the management platform, please use the platform to manage all personnel and local face management is not supported.

Tap **Settings** > **Face management** to manage facial images on device locally.

Add person

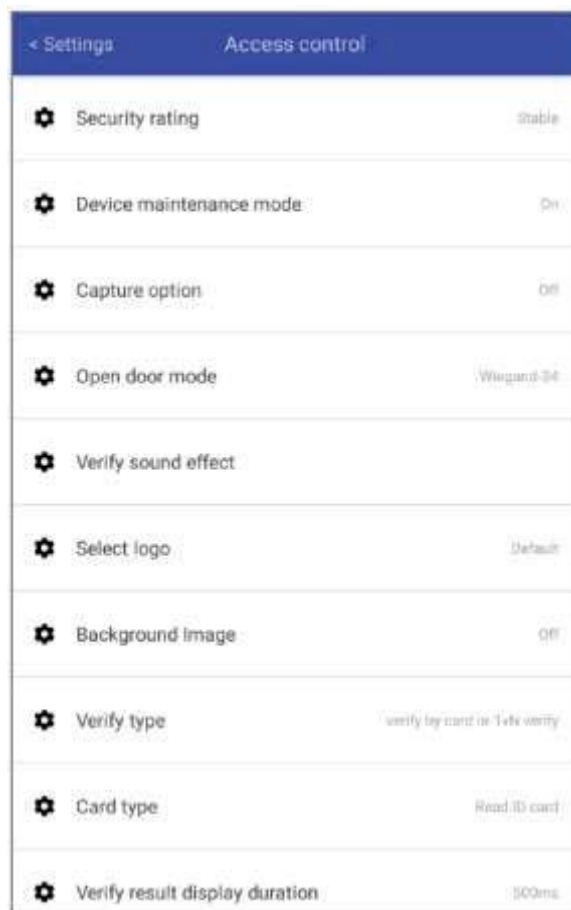
1. Tap ADD PERSON and tap the round icon in the center to take a picture. Please make sure that there is only one face in the center of the screen and do not take photos in backlight or poor light conditions. Your face should not be obscured.
2. Enter name and the 10-digit card number in the Create record dialog and tap CONFIRM to complete the new person addition.

Delete person

Select the faces you want to delete in Face Management page, tap Delete on the top-right corner and confirm to delete the face from the database.

4.2.3 Access control

Tap **Settings** > **Access control** to configure access control parameters.



Security mode	Support balanced liveness detection strategy, offering desirable precision and speed
Device maintenance mode	Once enable this mode, all alarm function is disabled. This mode is used to prevent false alarms caused by equipment maintenance or mis-operation. The device maintenance mode is enabled by default.
Custom capture parameters	Once enable these parameters you can set face image size and face detection area on a screen. Click CONFIRM to restart for the changes to take effect.
Communication settings	Select from Relay Output, Wiegand 26, Wiegand 34 and Network. Relay Output: When there is a door-open operation, the relay will close. You can specify the relay switching time that is the duration of the electric lock action to drive the door open. The default value

is 500ms.

Note: If the time is too short, the electric lock switch will not be triggered. If it is too long, the inner coil of the electric lock will be charged for a long time and the coil will burn out because of overheat.

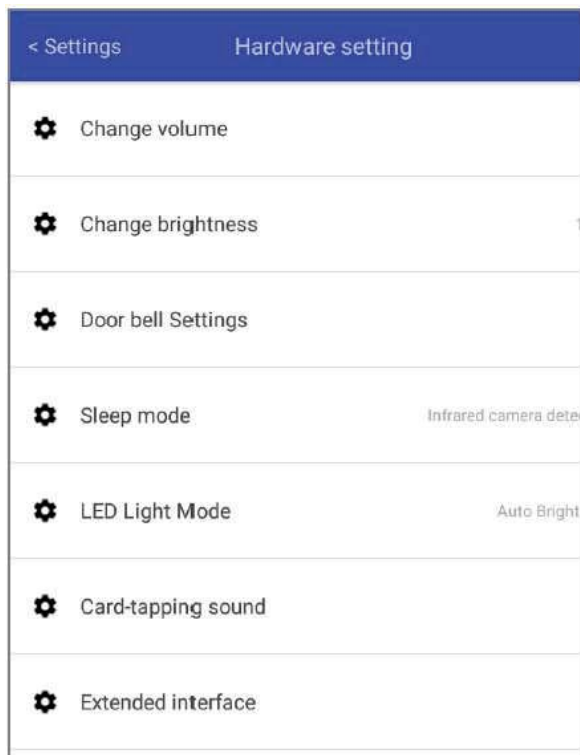
To connect with electric lock directly, make sure the supply voltage of the electric lock is <16V and the peak current is <2A.

- **Wiegand 26/34:** Send comparison results via Wiegand protocol. The data transmitted by Wiegand is the user card number obtained by comparing faces (this card number can be synchronized through the management platform data, and can also be set locally in offline state)
- **Network:** You need to set the IP address and the communication port of the management server.
- **Off:** Door-open signal will not be output in any circumstance even if the verification is successful.

Sound effect	You can set the sound effects for successful verification, failed verification and for the situation that access attempt is successfully verified yet does not meet a specific access policy. You can also upload customized sound effects via the tool provided. All sound effects are turned off by default.
Logo	The users can customize the logo or disable displaying logo.
Background	You can customize the background image or switch off the background image.
Comparison method	• Verify by card or 1vN Verify: 1vN matching by card or by face. • Verify by card + 1v1 Verify: 1v1 matching that verify card to identify the person, and then match the face to the identification. ⓘ Note: Remote retrieval mode does not support 1 v 1 verify mode.
Card type	The user can select from two modes: Read IC card and Stop Read IC card. ⓘ Note If the user selects Stop Read IC card, the card-reading function will be disabled on the device.
Verification result display duration	After a verification is successful, the relevant prompts and user names will be displayed on the capture interface. Here you can set the time duration of the prompts and user names. The default value is 500ms.
1vN matching threshold modification	By changing the matching threshold, the false alarm rate and the pass rate will decrease as the threshold increases. The default threshold is 85. You do not need to change the threshold if not necessary.

4.2.4 Hardware setup

In the **Settings** page, click on the **hardware setup** for hardware configuration.



Change volume	Adjust the speaker volume of the device
Change screen brightness	Adjust the screen brightness of the device
Change fill light brightness	Adjust the brightness of white light fill light
Modify brightness of infrared fill light	Adjust the brightness of infrared light fill light
Sleep mode	Set the device display off or reduce brightness of the screen when no one is detected. You can also set the screen to stay on. - time to turn off display: during which time if nobody is detected, the device will enter sleep mode automatically - screen brightness during sleep: set the screen brightness for the device in sleep mode - fill light brightness during sleep: set the brightness of the fill light when the device is in sleep mode
Fill light setting	Set the fill light to automatically adjust mode to normally turn on, or

normally turn off, according to the environment,

Switch sound	of	swipe
-------------------------	-----------	--------------

Decide whether the device has a sound after the user swipe the card

After opening, you can monitor the contact status corresponding to the digital signal input interface, and you can also configure the extended function of the interface according to the type of sensor connected

- **common sensor monitoring**

The device directly reports the detected contact status without any logical judgment.

- **Single door monitoring**

To use the single door monitoring function should make sure that the door opening mode is to relay output (Settings>Access control settings> door opening method> relay output).

- **The sensor of the door detection:** Set the working behavior of the connected door sensor: normally open or normally closed.

Normally open mode: When the door is open, the door magnetic probe is not close to the magnet and the device is in the disconnected state; when the door is closed, the door magnetic probe is in contact with the magnet and the device is in the conductive state.

Normally closed mode: When the door is open, the door magnet probe is close to the magnet and the device is in the conducting state; when the door is closed, the door magnet probe is not close to the magnet and the device is in the off state.

- **The detection of the door-opening button:** Set the working behavior of the door-opening button: normally open or normally closed.

Normally open mode: When the door open button is not pressed, the contact is in the disconnected state, that is, a door opening action in the door will detect the state change of the contact from open to conductive.

Normally closed mode: When the door open button is not pressed, the contact is in a conducting state, that is, a door opening action in the door will detect the state change of the contact from on to off.

After the device detects the door-opening action of the door-opening button according to the setting (the state change from disconnection to conduction or conduction to disconnection), it automatically completes the drive of the

Extensible API

door opening relay, and the continuous driving time is subject to the door opening setting time.

- **Intrusion alarm:** After opening the function, if the door is not opened by normal operation (such as opening the door by swiping the face or card, opening the door by the button, or remotely opening the door), the device will issue an intrusion alarm. Enter a valid user name and password to log in to the system to clear the alarm.
- **Door normally opened alarm:** After opening the function, after the door is effectively opened inside or outside, if the door-opening time exceeds the setting, the device will issue a reminder or alarm of the opening door, which will close as the door closes. The user can set the alarm time
The prompt time of the opening door: if the opening time of the door exceeds the set value, the device will give a prompt, the default is 20 seconds, from the last door opening time
The alarm time of the opening door: when the opening time of the door exceeds the set value, the device will give an alarm, the default is 30 seconds, counting from the last door opening time.

- **Serial communication:** The multiplexed contact interface is serial RS485 communication and used only for customized projects

Device restart	scheduled	Based on project needs, set a time for the device to restart everyday
-----------------------	------------------	---

4.2.5 Network settings

Click Network Settings on the Settings page to set up the network connection.

Set the method of getting IP to DHCP or static IP.

- LAN settings**
- **DHCP:** The device automatically obtains an IP address.
 - **Static IP:** Enter the IP address, subnet mask, and gateway address manually.

Wi-Fi	Select the wireless network to connect, or add the network manually.
--------------	--



Description

If you want to connect to the management platform, it is necessary to ensure that the device and the management platform are interoperable.

You can discover and manage devices in the management platform. For details, please refer to the management platform user manual.

4.2.6 Surveillance information

Clicking the Monitoring Information on the Settings page, you can view the current terminal portrait library information and historical comparison data.

< Settings		System statistics
⚙	Database version	dab4079bf5ab53a9603f5a3fb25ed874
⚙	Person(s) in total	1
⚙	Verification time(s) in total	0
⚙	Successful verification in total	0
⚙	Refresh	

Version information

of a face image database The current personnel database version on the device.

Person number of a face image database The total number of face records in the database of the device.

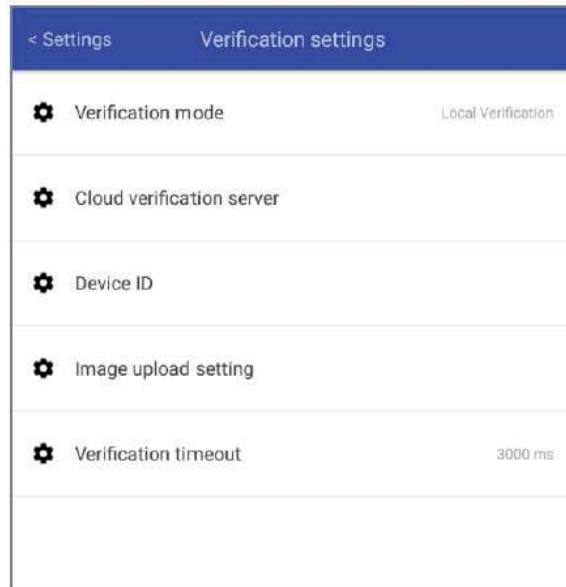
Total verification times The total number of verifications the device has done.

Successful verifications in total The total number of pass signal that the device has sent.

Refresh Refresh the data

4.2.7 Verification settings

On the Settings page, click the comparison setting, you can choose the comparison method (local or remote), capture the uploaded content, timeout, and set the back-end server to connect the device to a third-party comparison platform.



- Verification mode**
- **Local verification:** The device compares captured face with the faces in the local database.
 - **Cloud Verification:** The device captures the facial image and sends the image to the back-end for comparison. According to the results of the back-end feedback, prompt information display and door opening operations are performed (swipe card + 1v1 comparison is not supported) .

Cloud verification server	The back-end comparison server address format is IP address: port number. You can also enter the server domain name directly. The URL is left blank by default.
Device ID	You can enter the corresponding information according to the requirements of different servers. The content of the ID is maintained in the json format. When the device is connected to a server to upload information, it will automatically bring the identifier content in string format without additional processing. The URL is left blank by default.
Image upload setting	Select the image type uploaded each time a face is captured. By default, only the captured image will be uploaded.
Verification timeout	Set the wait time for the data uploaded to the back-end platform. If exceeding the time limit, a failure will be reported. The default value is 3000ms.

4.2.8 Human body temperature measurement settings

Add Infrared Thermal Imaging Module (YT-STX82-APHG), click the human body temperature measurement setting on the settings page to configure the temperature measurement function.

Temperature module status	• Not connected The connection of YT-STX82-APHG temperature measurement module is not detected. • Connected It is detected that YT-STX82-APHG temperature measurement module works normally.
Detection mode	When the temperature measurement module is connected normally, you can choose whether to turn on the human body temperature measurement function.
Access mode	• Temperature check + Facial check Only when the validity of the user's face and the user's temperature are within the alarm temperature, the pass judgment result can be given. • Temperature measure & Facial check Only the validity of the user's face is judged as a pass judgment, and the corresponding prompt will be given according to the detected user's body temperature. • Temperature check Pass judgment is given only through the results of human body temperature measurement, without judging the validity of the face.
Temperature unit	When reminding the user of the temperature measurement result, the temperature unit used supports Celsius and Fahrenheit. The default is Celsius.
Display modes	• Show Thermal In the using state, real-time infrared thermal imaging map will be displayed at the same time. • Normal operation Keep the original interface unchanged without infrared thermography. Default is Show Thermal mode
High temperature alarm	When the temperature of the user's face is detected to be higher than the alarm temperature, the high temperature alarm prompt will be given. The default is 37.3 °C

4.2.9 About

Check the software version of the current device at the Settings> About menu.

5 platform to access

The device can be connected to MacroEye Platform in two ways: active and passive, to realize personnel data synchronization, personnel batch storage, visitor management, attendance statistics, device deployment and other functions.

Cautions



Please make sure network connectivity between the terminal and platform server is normal.

If the terminal has already been added on the platform, and needs to connect to the platform actively, please remove the terminal from the platform in advance.

5.1 Active connection

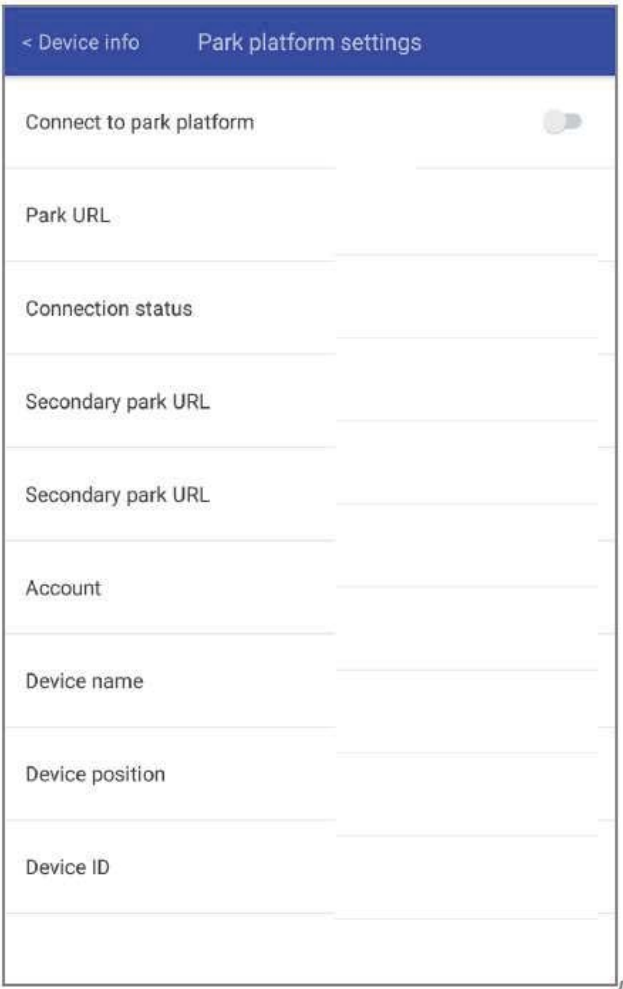


Cautions

Please ensure that the version of the campus platform supports active access

The steps for the device to actively access the campus platform are as follows:

1. On the Settings page, click Device Information> Campus Settings.



2. Turn on the switch of active connection campus setting, and make corresponding settings in the pop-up window.

Park address / backup park address The network address of park platform server that could be IP address: port number or a domain name. The default port number is 8049.

Verification code To access the verification code of the campus, you can go to Platform Management> Device Management in the campus management platform and click the verification code to view. The verification code is dynamic and valid for 24 hours

If the park has not been activated and the verification code cannot be obtained on the page, the implementation personnel need to provide the initial verification code, please refer to the park implementation manual or consult the implementation personnel

Account/password	The account and password for the device to access the park are provided by the implementation staff
Device Name	Define the name of the device to distinguish it
Device Location	Define the location of the device to distinguish the device

When finished, click OK, and the device will try to access the campus. If you successfully access the campus, the campus connection status on the campus settings page will display the campus connection, as follows:

If the connection is unsuccessful (invalid address, network error, abnormal connection, etc.), the setting button on the standby interface will display red  and after a normal connection, the button will return to gray.

On the device management page of the park management platform, the device status will also be displayed. Please refer to the corresponding park user manual for the operation of the equipment at the park

5.2 **Passive access in the platform**

The terminal can be detected and connected on the park platform side. Please refer to the relevant park platform operating manual for details.

Appendix Proper Nouns

Smart Facial Recognition Terminal

A device that is equipped with a dual-lens camera, an 8-inch touch screen and an Android system. The terminal is installed outside the door that it is connected with and captures and compares the face. According to the comparison result, a control signal would be sent to the electric door, and the access record will be saved at the same time.

Management Platform

Installed on PCs or servers, the software can connect all terminals via local area network and thereby create, read, update and delete the face database on all terminals. You can also view the pass records on terminals via the management system.

Record

Each time when a terminal captures a face, a record will be generated after a comparison is done. The record includes information like pass time, device name, captured photo and the information of the person who passed the door, such as name, employee number, etc.

Access control /Access control unit /Access controller

The unit is used to receive the signal from the terminal. If the signal is to open the door, the door will be opened; if the signal is not to open the door, the door will not be opened.

Dual-Lens camera

Two lenses are installed within the camera: visible light lens and infrared lens. The latter one is used for system-assisted imaging and liveness detection under the condition of poor light.

Wiegand

The Wiegand protocol is a protocol that converts a card number into a string of binary signals. If the card number is 26 bits after conversion, it is called Wiegand 26; if it is 34 bits, it is called Wiegand 34. These two formats are the most commonly used.

IC Card

IC Card (Integrated Circuit Card) is a physical electronic authorization device, used to control access to a resource. It is readable, writable, has large capacity and can be encrypted. Also, its data record is reliable. Applications include access control system, consumer system and so on, such as bus cards and bank cards.

Face capture

The step before facial recognition, which is to accurately mark the face position in the photos taken by the camera.

Liveness detection

The facial image captured by the camera equipped with a visible light lens and the infrared light lens will be analyzed by the deep learning algorithm. The algorithm will judge if it is a human being's photo. Only in the case that it is a real person, the algorithm will compare the photo with a data- base.

Facial feature extraction

Features that can be used by the face recognition system are generally classified into visual features, pixel statistical features, face image transform coefficient features, and face image algebra features.

1: N and 1:1

- 1:N matching - The comparison between facial images captured by the device and images in the database.
- 1:1 matching - The comparison between the information interpreted at card tapping and the corresponding information in the database.

Generally speaking, 1:1 is used to identify if the photo taken is you while 1:N is used to identify which one is you.

False rate

Identify two photos of different people as the same person. The 1:1 false alarm rate and the 1:N false alarm rate can be converted, and the formula is:

$$1:N \text{ False Alarm Rate} = 1:1 \text{ False Alarm Rate} \times N$$

Pass rate (acceptance rate)

Unlike false rate, the pass rate will not change as the size of the database changes and the formula is therefore:

$$1:N \text{ Pass Rate} = 1:1 \text{ Pass Rate} \times N$$

Threshold

The essence of the comparison is to calculate the similarity score of two facial images by artificial intelligence algorithm. By comparing the similarity score with the threshold, the algorithm will get the comparison result. If the similarity score is higher than the threshold, the two facial images are considered to be the same person, and vice versa. The threshold determines the false alarm rate and the pass rate. That is, the higher the threshold, the lower the false alarm rate and the pass rate will be; or the lower the threshold, the higher the false alarm rate and the pass rate will be.

To measure the quality of an algorithm, you can compare either the pass rate at the same false alarm rate or the false alarm rate at the same pass rate. The former one is more commonly used.