ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 5, Issue 4, pp: (22-26), Month: October - December 2017, Available at: www.researchpublish.com

# Design and Implementation of Intelligent Lock based on IOT

[1]Baocong Liu, [2]Chenyu Liu, [3]Hao Chen, [4]Suhang Guo, [5]Wenying Li, [6]Ling chao Zhao, [7]Ziling Feng

[1234567]Electronic and Information Engineering, Tianjin Polytechnic University, Tianjin, China

***Abstract:*** **In order to solve the problem of the existing security risks of electronic password lock, the article is designed to combine electronic code lock and Internet of Things technology to form an electronic code lock based on IOT. The electronic code lock is based on FPGA, the real-time acquisition and transmission of network video is realized based on Da Vinci technology TMS320DM368 processor hardware platform. The design of the password lock in addition to a lock, unlock, clear, password reset, the system alarm function, in the two consecutive input password error, will trigger the network video capture transmission system, and notify the user password lock malicious intentions, when the third password input error, the password lock into the deadlock and alarm.**

***Keywords:*** **Internet of Things, FPGA, Electronic Locks, Network Video Transmission.**

## 1. INTRODUCTION

Combination lock is most commonly used in commodity management security tool, and the development of the digital combination lock in the information age is becoming more and more quickly. Although the safety performance is gradually improved, it is still pose a safety hazard. If the lock and the IOT are combined, at the same time monitor the environment around the lock when the password appears certain number of errors, timely remind users that the password lock has security problems so that users can respond to the security problems of the code lock in a timely manner and can also take evidence of the perpetrators. Therefore, further research on the application of IOT in digital cryptography locks could make great social and economic significance for further enhancing the security mechanism of cryptography locks.

## 2. SYSTEM DESIGN

Combination lock based on IOT is mainly composed with two parts, first part is the electronic trick lock based on the FPGA , the basic functions can complete the password input, clear, remove, change, lock and unlock, there are two levels of password management mechanism; The other part is the network video acquisition and processing transmission system based on the TMS320DM368, the main function is to obtain the video data collected by the image sensor, and then encode the file of h.264 format through the video encoder. Finally, the streaming server forwards the compressed packets to the client via the RTSP/RTCP/RTP protocol.

The overall system architecture is shown in Fig.1. Complete the password input and display through the HCI interface, When password mistyped two consecutive times will generate a trigger signal, trigger forward network video acquisition system, and the current image will collected and encoded to the server side, at the same time send warning information to the client through the server.

ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 5, Issue 4, pp: (22-26), Month: October - December 2017, Available at: www.researchpublish.com

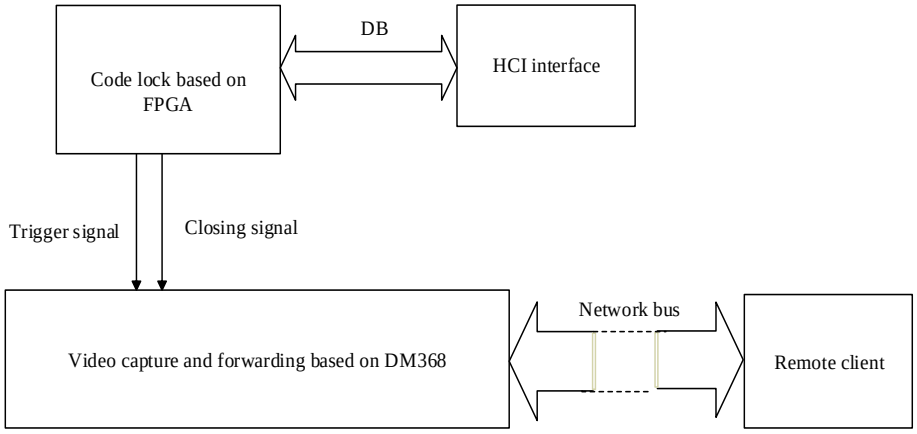


**Fig.1 System architecture**

## 3. DESIGN AND IMPLEMENTATION OF PASSWORD LOCK

The password lock system designed in this paper is mainly composed of four modules: HCI interaction module, counter module, password management module, the main controller module, the structure diagram is shown in Fig.2. Mark 1 is the core part of password lock security mechanism, that is, password management module, in which the main functional modules are cipher encryption algorithm implementation module, password storage register module and so on. Mark 2 is the control state conversion module of the whole operation mechanism of the cipher lock, which completes the state transition by receiving the parameter signals inputted by the user interface.

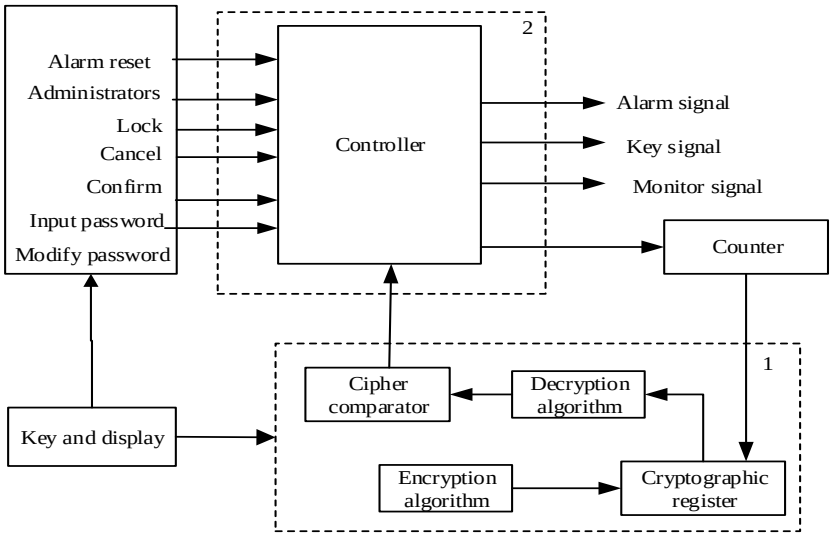


**Fig.2 Block diagram of cipher lock**

### *3.1 Encryption module:*

The principle of mask encryption is that each bit M of the original four bit unlock password is implemented with the same unknown mask sequence C, and the result is stored as the key in the password register module. The traditional encryption algorithm is low memory and security, so this paper uses a multi bit improved mask encryption algorithm to upgrade the mask to 4 bits and sixteen hexadecimal numbers, the original four bit cipher is encrypted with different 4bit binary numbers. This is because of the mask is 4 sixteen hexadecimal data, even acquire the cipher text, there are 16 kinds of mask for each calculated password, so there are $16^4$ types of masks. The probability of a password being deciphered is $1/16^4$, a relative mask code breaking rate is reduced by $16^3$ times. This topic chooses to use 4 bit sixteen hex mask to encrypt, its mask mode is XOR operation, and the security of the encryption method is analysed, it is found that any sixteen decimal number is zero to its own XOR. Finally select 1010 1011 1100 1101 as the four bit sixteen hexadecimal data as mask. After simulation test and analysis, the encryption effect is better.

ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 5, Issue 4, pp: (22-26), Month: October - December 2017, Available at: www.researchpublish.com

### *3.2 Master controller module:*

The main controller circuit module is the important part of the password lock. Using Mealy type finite state machine to control the switch state selection of password lock, and one-hot code encoding is used to state encoding, in order to simplify the state conversion circuit. One bit code is used to implement N state machine with N flip flops, in this way, it can not only simplifies the state decoding logic, but also speeds up the conversion speed of the state machine. In the implementation, the Verilog description is described by a single process. The state and sub states of the state and the input and output logic are described in an always process, so that the circuit can be simplified.

Fig.3 is a lock state transition diagram. The initial state is locked state (In_lock), in this state, pressing the start button to enter the password input state (Password_input), if the password is correct, enter the correct password state (Password_right), in the state of unlocking password if you press to modify password status (Password_change). In the password input state, If the password goes two times wrong, there will produce a trigger signal, three times wrong will goes into a deadlock state alarm (Warm_lock), press the button to enter the administrator state and administrator (Admin_state) can reset the system.

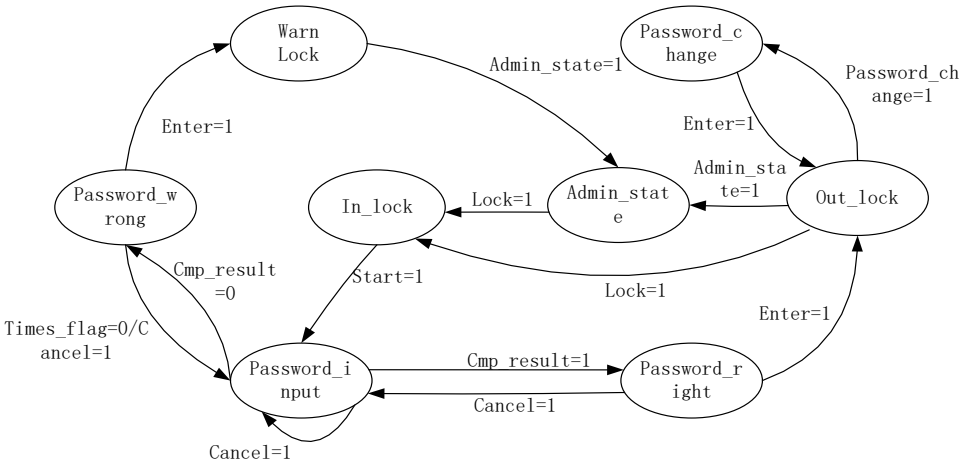


**Fig.3 The transition of password lock state**

## 4. NETWORK VIDEO TRANSMISSION SYSTEM

The system uses TMS320DM368 as the main processor of the network video monitoring system, and the design structure is shown in Fig.4. Based on digital media processor, its internal structure is ARM+DSP structure, ARM is to complete the function of control, the DSP processor to complete the video data encoding, flash storage software system, DDR system for processing data. The peripheral equipment structure used to support other camera access processor. Video transmission scheme to transmit video data is through the RJ45 cable crystal head. Live555 media streaming server is built internal embedded processor.

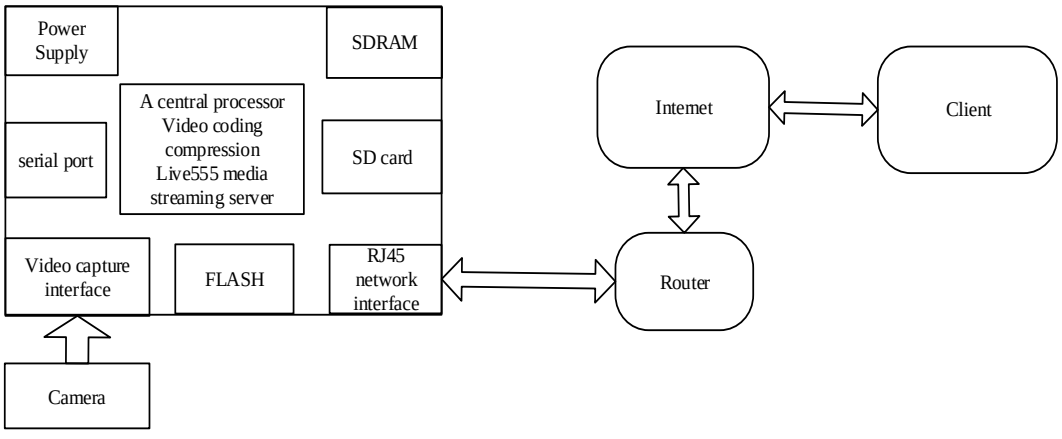


**Fig.4 Network video transmission system**

### *4.1 Design of video capture and coding program:*

The program is composed of four threads: the Capture thread for video capture, the Video thread for video coding, the Written thread for video storage and Main thread. The DM368 video capture program is based on the V4L2 library function under the Linux system, and V4L2 provide a set of interface functions developed for the driver by using a layered method. Only the developers need is to call the V4L2 provided by API, the video capture function application could rapidly implementation. Video coding is realized by calling Codec Engine's VISA interface function. The video data is compressed by H.264 encoding, and then the encoded data is stored as a shared file for the streaming media server to read the data.

### *4.2 Transmission module of H.264 video stream:*

The RTP transmission module of H.264 video stream is responsible for encoding the video stream according to the RTP H.264 packet strategy video stream packaged into RTP packets, and then sent to the remote client program, this program using streaming media server to complete the real-time broadcast video files.

Live555 is a real-time media data streaming server based on C++. It implements the media stream transport protocols such as RTP/RTCP, RTSP and other standards. When the client sends a request to the server, established a connection with server and client, the client sends video on demand, real-time video encoding server reads the *.264 file into RTSP data stream transmitted to the client. When the client is connecting, only the client needs is in the same LAN with the network video acquisition and transmission system, can view the current monitoring screen, and access the video capture server address by using VLC multimedia player.

## 5. TEST RESULTS

Video capture and transmission test results, as shown in Fig.5 for the client monitoring picture, Fig.6 is the network video transmission system to achieve real-time video capture, transmission, scene display. The resolution of the video is 720p/30fps, the video data compression rate is 2M bit, the monitoring screen is continuous with the actual scene video frame, but there are 2~3 seconds delay.

Integrated test with the password lock system and network transmission system. When in the two consecutive input password error, will triggering video acquisition and transmission system to open the monitor, the cache monitor screen will be transmitted to the streaming media server, client can access monitoring screen by accessing server address.

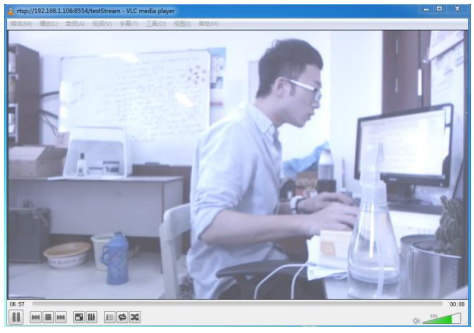

**Fig.5 Client monitor screen**

**Fig.6 Real time monitoring scene mode**

## 6. CONCLUSION

This design has completed the basic function of the electronic password lock based on Internet of things, the lock, unlock, modify password, alarm deadlock and administrator reset system function can be realized on EP4C10F17C8N. For the network video acquisition and transmission system, it can complete the video stream collection and real-time forwarding in the TMS320DM368. The client can access the server address through the VLC multimedia video player, receive the real-time video data stream and display. This design combines the network video transmission technology and the electronic password lock, and makes up the security hidden trouble of the traditional electronic password lock. Make the system safe and stable operation by using Linux ARM embedded operating system, at the same time small streaming media server in embedded built to complete the real-time video transmission network, as long as the client access to the server in the LAN can access the server address to see real-time video surveillance.

## REFERENCES

[1] Yigen Rui, "Design and implementation of conference terminal software for embedded video conference system", Nanjing University of Science and Technology. 2008.

[2] Codec Engine Application Developer's Guide, Texas Instruments Incorporated. 2009.

[3] Bibo Yan, Zhengbing Zhang, The video acquisition and transmission system based on ARM, China high-tech enterprise, 2009(4):52-54.

[4] Da Vinci Multimedia Application Interface User Guide. Texas Instruments Incorporated, 2009.

[5] IPNC Reference Design on DM36x Application Design Guide, Texas Instruments Incorporation, April 2010, 20-60.

[6] Yulong Fan, Ming Yang, Hu Zhang, Design and implementation of high definition video transmission system based on TMS320DM368, Journal of Ningbo University. 2014 (1): 53-56.

[7] Lianhua Li, Design of electronic password lock based on FPGA, Chinese science and technology information. 2006 (1): 63-63.

[8] Yanfei Mao, Design and implementation of network video surveillance system based on RTSP protocol and H.264 coding, Zhejiang University. 2011.

[9] Shaozhong Hu, Development of embedded video surveillance system based on Linux, Anhui University of Science and Technology of China. 2009.5.

[10] Wei Song, "Design and implementation of HD network camera based on TMS320DM368", University of Chinese Academy of Sciences. 2013.

[11] Song Zhan, "Design and implementation of wireless video monitoring system based on DM368", Wuhan Institute of Technology. 2015.

[12] Zhen Li, Guoyu Wang, Design of reliability electronic code lock based on FPGA, Modern electronic technology. 2013(7):151-153.

[13] Mingxi Li, Design of new electronic code lock, development and innovation of mechanical and electrical products. 2004, 17(3):40-40.

[14] Janming Chen, Yixiang Zhang, Study of streaming media server for mobile learning, Microcomputer and applications, 2013, 32(3):10-12.

[15] Jin Zeng, "Design and implementation of embedded streaming media server", Nanjing university of posts and telecommunications. 2011.

[16] Wensheng Wu, "Software system design and implementation based on DM368 high definition IP Camera", Huazhong University of science and technology. 2011.

[17] Bo Zheng, "Research and implementation of encryption algorithm based on FPGA", Jiangsu university, 2008.

[18] Jianxun Song, "Design and implementation of video monitoring system based on Da Vinci technology", Nanjing University of posts and telecommunications. 2011.

[19] TMS320DM36x Digital Media System-on-Chip Video Processing Back End User's Guide, Texas Instruments Incorporated. 2009.

[20] Yaoxing Huang, The field programmable gate array performance is first explored, Silicon valley. 2011 (5) : 193-193.

[21] Guangran Liu, FPGA primer step analysis, New course study. 2014(6):131-131.

[22] Da Vinci Linux VPIF Display Video Driver User's Guide, Texas Instruments Incorporated. 2009.