Design of Embedded Audio Encryption Communication Equipment Based on Bluetooth

Liangliang Li[1, a], Zhigang Lv[1, b], Yongxia Yang[1, c], Yiguo Huang[1, 2, d]

[1] School of Electronics and Information Engineering, Xi’an Technological University, Xi’an 710021, China;

[2] No.3 Research and Development, Jiangsu Wireless Telecom Plant Co. Ltd., Nanjing, 210012, China

[a] 2977867201@qq.com, [b]619555658@qq.com, [c]1971201818@qq.com, [d]957737074@qq.com

Keywords: CSR8670; STM32F103C8T6; MX128; Audio encryption.

Abstract: For the security problem that the content of audio call is easy to be eavesdropped, this paper introduces an audio encryption communication device for mobile communication terminal. The system is mainly composed of two core processors CSR8670 and STM32F103 and its peripheral hardware circuits. The CSR8670 implements a link connection between a mobile phone and a device for transmitting audio data. The STM32F103C8T6 is used to implement intelligent control and data processing functions for the system. The audio encryption module adopts a low-power audio encryption dedicated chip MX128, and realizes the function of audio encryption and decryption by designing a hardware circuit. Through many experimental tests, the device can realize audio encryption communication between different mobile phones and different mobile networks.

1. Introduction

With the rapid development of mobile communication industry, voice communication is becoming more and more popular in people's life. However, when people use mobile phones and other mobile communication devices to bring convenience, there is also a potential threat. One of the security problems in voice calls is that the content of voice calls is illegally intercepted and monitored. Voice communications often contain important information, such as personal privacy, trade secrets or even military secrets related to national security. If information was leaked, it will cause great losses to the interests of individuals or groups. [1] In this paper, The author use the principle of signal source encryption, make the voice of the mobile terminal equipment has already been encrypted, voice out decrypted by the device after the mobile terminal, to ensure the cipher-text state in the whole mobile terminal[2].

2. System design

This paper mainly researches a kind of communication equipment with voice encryption function. Through the analysis of the system’s requirements, the author completes the system scheme design of the equipment. The device supports plaintext communication and cipher-text communication. The overall block diagram of the system is shown in Figure 1.

3. System hardware design

In this paper, this system is mainly composed of two core processors, CSR8670 and STM32, as well as its peripheral hardware circuit. STM32 and CSR8670 Bluetooth module are used for data communication through wireless link. The advantages of STM32F103C8T6 are embodied in the operating frequency can reach 72MHz, which meets the design requirements of the system[3].CSR8670 blue-tooth chip can be secondary developed through the software development platform Blue-Lab, and its chip is integrated with MCU and CODEC modules [4].The basic function of the audio blue-tooth module is to establish a wireless communication link between the mobile phone and the device to transmit voice data[5].

STM32 is in the working status of reading the Bluetooth module, and displays the read data on the LCD in real-time. Data communication between STM32 and LCD through I2C can display system clock, call number and call status in real-time. STM32 controls the encryption module, MX128 that through the original high frequency shift to the low frequency band, low frequency band is moved to the high frequency band, Thus the spectrum of the original speech signal is scrambled [6][7], In the design, encryption or decryption is operations by reading the status of the key module; The power module,NCP500-3.3, provides 3.3v voltage to STM32 to ensure its normal operation. The hardware design block diagram is shown in Figure 2.

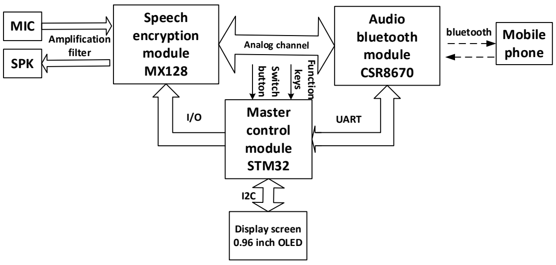

MIC
SPK
Amplification filter
Speech encryption module MX128
Analog channel
Audio bluetooth module CSR8670
bluetooth
Mobile phone
Switch button
Function keys
I/O
UART
Master control module STM32
I2C
Display screen 0.96 inch OLED

Fig.1 overall block diagram of the system

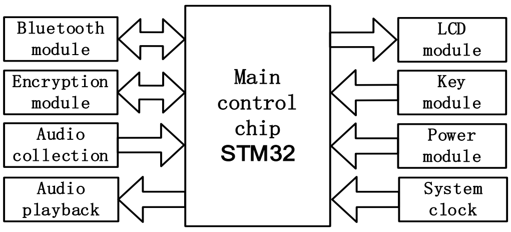


Fig.2 block diagram of hardware

4. System software design

The software used in this paper is Keil µVersion5, on this platform, programs can be programmed through the STM32 firmware library.[10] The software design is shown in Figure 3.

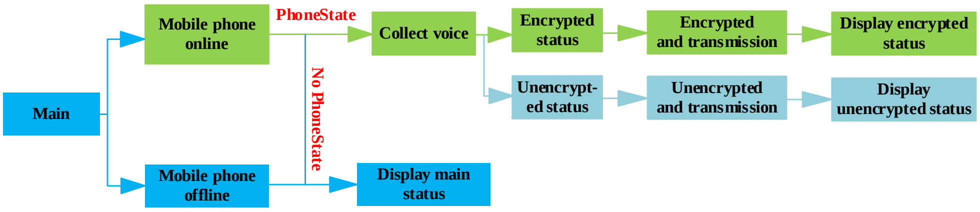


Fig. 3 system software flow chart

5. System testing and result analysis

In this paper, by building two groups of test platforms, the equipment has been tested for many times, and the test results have been evaluated and analyzed. The specific test process is as follows:

1) Standard non-speech signal test

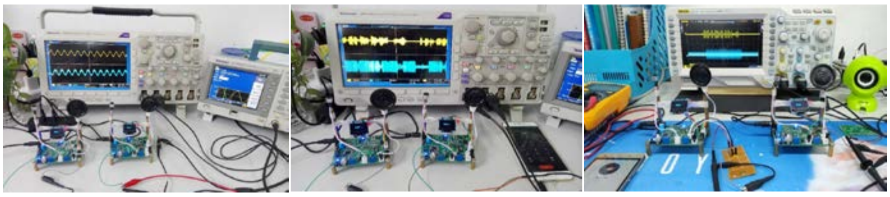
As shown in Figure 4(a) is composed of signal generator and oscillograph test environment, This environment is mainly used to test standard non-speech signal after the equipment amplification, filtering, encryption and other processing through the mobile phone transmission to the GSM/CDMA mobile network, the mobile network will encode and decode the signal, and the signal waveform at the receiving end will be consistent with the original signal waveform after being decrypted by the device.

2) Standard speech signal test

As shown in Figure 4(b) is composed of sound source and the oscilloscope test environment, the upper waveform of the oscilloscope is the input waveform of the voice signal, the voice signal is the standard voice generated by the mobile phone as the sound source, and the lower waveform is the output waveform of the receiving device, pass the test can be found that the receiver equipment of the output waveform has not weaken and disappear, and the waveform change and input waveform change is basically the same, with only slightly magnified and delay, and the waveform’s delay no more than 150ms.

3) Standard speech signal encryption test

As shown in Figure 4(c), the waveform above the oscilloscope is that device 1 (the sender), which inputs a speech waveform reading 1 to 9 through the microphone interface, while the waveform below the oscilloscope is that device 2 (the receiver) outputs the speech waveform through the speaker interface after encryption. From the waveform displayed on the oscilloscope, it can be seen clearly that the encrypted speech signal waveform is similar to white noise, which completely losing the features of speech, without any information, thus achieving the encryption effect and meeting the system design requirements.



(a)standard non-speech signal test (b)standard speech signal test (c)standard speech signal encryption test

Fig.4 system test

6. Conclusion

Aiming at the security problem of voice communication in current mobile communication system, this paper designs an embedded blue-tooth voice encryption communication device based on mobile terminal communication security. Finally, the experimental test was carried out in the laboratory environment, and the experimental results were analyzed. The experimental results prove the feasibility of the design. This device is suitable for a variety of mobile terminals such as mobile phones with Bluetooth function, this device doesn’t need any software and isn’t limited by any operating platform. It is convenient to use and have certain practical value.

Acknowledgements

The authors gratefully acknowledge the financial support from Scientific Research Program Funded by Xi'an City Weiyang District Science and Technology Department (201923) Shaanxi Province, China.

References

[1] Han Xin zi. Research on end-to-end voice encryption and transmission technology for mobile communication [D]. Nanjing: southeast University, 2016.

[2] Dong Xiao Ping. Phone call security encryption technology research and analysis [D]. Wuhan, China: Hubei University, 2013.

[3] Li Jian-hui. The Design of Embedded Audio Communication Equipment Based on Bluetooth [D]. Tianjin: Tianjin university, 2004

[4] Jiang Song-qi. The Design and Implementation of Bluetooth Headset Based on CSR8670 [D]. Nanjing: southeast University, 2015.

[5] John Paul Dunning. Taming the blue beast: A Survey of Bluetooth-Based Threats [J]. Security & Privacy, IEEE, 2010:3-17.

[6] Liu kai hua, Sun Sheng ju. The Design of Voice Scrambling Module Based on Wireless Data Transmission Technology [J]. Application of electronic technology, 2007.

[7] Li Wen juan. A Study of Encryption Technology Based on the Analog Voice [D]. Xi’an: XIDIAN UNIVERSITY, 2014.

[8] Shuai Jiang hua, Li Zhi yi. Discussion on the application of LM386 amplifier in practice teaching [J]. Wireless interconnection technology, 2016, 0(24): 125-126.

[9] CSR, CS-309942-UGP3_ADK Configuration Tool User Guide, 2014:7-17.

[10] Li Jian-hui. The Design of Embedded Audio Communication Equipment Based on Bluetooth [D]. Tianjin: Tianjin University, 2005.