Research on Jamming the Recording Device through Microwave Radiation

Zeng Chuyang, Gao Shang, Xiao Jianyi, Huang Jianwen, He minnuo, Lin Qiang, Huang Kaitong, Huang Jutao, Ma Ruiwen

Information Centre, Guangdong Power Grid Corporation, Guangzhou, Guangdong, 510000, China

Keywords: Research, Jamming, Device

Abstract. The principles on jamming the recording device using the mobile communication GSM signals are analyzed. An idea is proposed to interfere the recording device through microwave radiation. The operating principles and defects of the recording device are discussed. The curve describing the variation in sound level readings with radiation parameters is quantitatively measured. Experiments are performed using the designed prototype. Results demonstrate the ability of the prototype to effectively suppress the normally recorded waveform.

Introduction

With rapid advances in information technologies during recent years, various methods have sprung up to steal secrets. Miniature eavesdropping devices and hidden cameras can disguise as glasses, vehicle keys, pens and buttons. Moreover, these devices are capable of wireless transmission and reception, posting a harsh challenge to the protection of national and military secrets as well as personal privacy. In this context, it is absolutely necessary to study how to keep audio and picture information from unauthorized recording. The operating principles of the audio recorder are discussed in this paper; a novel idea to jam the audio recorder is proposed. Experiment is performed to evaluate the ability of the designed prototype to interfere a recorder. Experimental results show that after receiving interference from microwave radiation, the waveform of the recorded signal is too distorted to be recognized.

Microwave is a common name of decimeter wave, centimeter wave and millimeter wave, referring to a limited frequency band in the radio wave. In other words, it represents the electromagnetic wave in the range 300MHz-300GHz, or the electromagnetic wave whose wavelength is no less than 1mm and below 1 m. The frequency of microwave is usually higher than the radio wave and it is thus called UHF electromagnetic wave. As a form of electromagnetic wave, microwave also exhibits wave-particle duality. The energy of microwave quantum is 199×l0-25 ~ 1。99×10-22j. The basic properties of microwave include penetration, reflection and absorption.

(1) Penetrative: microwave is more penetrative, because its wavelength is longer than other electromagnetic waves used for radiation heating, like the infrared ray and far infrared ray.

(2) Adjustable: the output power of the microwave can be adjusted anytime, making it particularly suited for automatic control and continued production. The microwave is usually generated by special devices involving direct current or 50MHz alternating current. It can be easily tested in the experiment.

Research Idea and Experimental Verification

The traditional magnetic tape-based recorder has become obsolescent and the market nowadays is dominated by the digital recorder. It is necessary to first analyze the operating principle of the jammed device. Generally speaking, the operating principle of the audio recorder can be explained as follows. The microphone works as a sensor to receive the sound signal, which is then amplified by the primary amplifier into voltage signal in the order of magnitude of mV. After AD sampling, quantification and coding, the voltage signal is converted into digital signal for storage. In order to play the recorded sound, the signal is processed by the sound decoding chip into analog voltage signal which is output by the loud speaker. Its working principles are shown in Table 1. Note that the microphone is key to electric-audio conversion, because the range and smoothness of its frequency response directly determines the quality of the subsequent recording process. Generally, the microphone in the high-end recorder is excellent in terms of sensitivity, frequency response and smoothness. After analyzing the wiring of several types of recorders, it is learned that the audio line connecting microphone with AD sampler is prone to be jammed. The external jamming signal is no longer effective once the electric signal is converted into digital signal for storage. Experiments are performed on different parts of the recorder by using the radio frequency probe as the interference source. The results indicate that the audio line at the end of the microphone is very susceptible to interference.

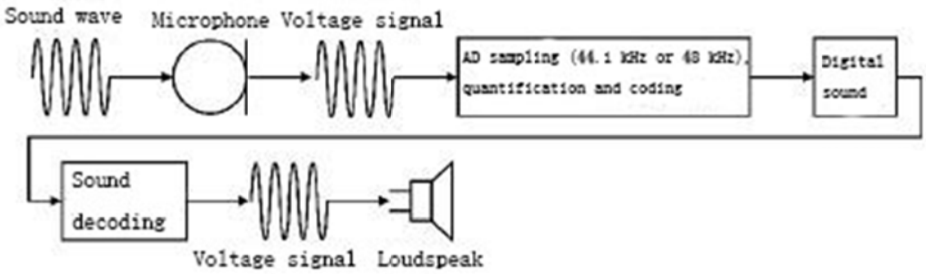

Fig. 1

Sound wave	Microphone	Voltage signal	AD sampling (44.1 kHz or 48 kHz), quantification and coding
Digital sound	Sound decoding	Voltage signal	Loudspeaker

It has been proven in the literature that when the GSM (Global System for Mobile Communication) mobile phones are calling or ringing, the audio devices nearby will beep. This is because the GSM mobile phones operate at a frequency band of 900MHz /1800MHz based on the TDMA (Time division Multiple Access) technique. Each channel occupies a bandwidth of 200 kHz and is divided into 8 slots and thus shared by 8 users. The mobile phone can only transmit signal during the slot allocated to it and it must shut down when the slot ends in order to avoid affecting users of neighboring channel. During normal operation, the GSM mobile phones send audio messages to the base station by transmitting pulses at a width of 577μs, radio frequency period of 4.615 ms and repetitive frequency of 216.7 Hz. The level of power output in the GSM mobile phone is adjusted by the power control signal from the base station. The mobile phone transmits the radio frequency pulses at the maximum output power after its connection with the base station is newly established. Therefore, when the mobile phone is calling or ringing, the radiation power is large and makes the audio devices susceptible to electromagnetic interference. Fig. 2 shows the simulation results regarding the time-domain waveform and its spectrum distribution after the GSM signal is processed through video demodulation. It can be seen from Fig. 2(b) that the principal frequency of the demodulated GSM signal is concentrated in the range within 3 kHz. This is the sensitive frequency band for the human eye and various audio devices. It can thus be inferred that transmitting the GSM signal through TDMA makes the audio amplifying circuit susceptible to be interfered by the external high-frequency electromagnetic field.

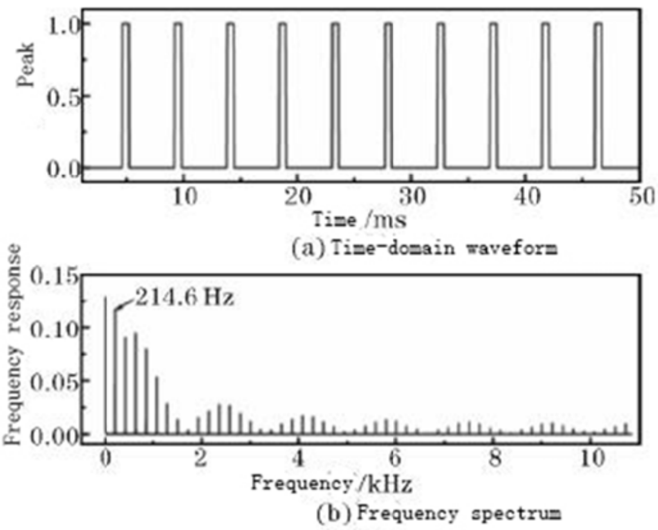

Fig. 2

Peak	Time	Time-domain waveform
Frequency response	Frequency	Frequency spectrum

Considering the grave difficulty in quantitatively estimating the level of influence on the audio device, the experiment is performed on sound level meter, which collects the ambient audio signal using the microphone. The collected signal is then processed to show the corresponding sound pressure level. In order to check the interfering influence of GSM signal on audio devices, the Agilent 8257D signal source and the Amplifier Research standard antenna are used to simulate the interference source of GSM signal. Experimental results show that after the sound level meter is exposed to electromagnetic radiation, the normal level of 55dB for the indoor background noise is increased to 90dB. This means that the signal processing circuit of the sound level meter is severely interfered. When the signal radiation frequency varies, the meter's reading fluctuates periodically. In order to study the influence of the wireless carrier's electromagnetic pulse on the readings, the Agilent 8133A pulse generator and the dipole radiation antenna is used for experiment, and the testing principle is shown in Fig. 3.

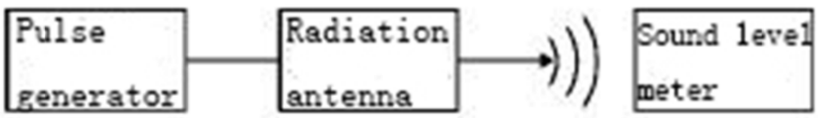

Fig. 3

Pulse generator	Radiation antenna	Sound level meter

Figure 4 (a) shows the variation of the readings with the electromagnetic pulse's repetitive frequency, where the pulse generator's output voltage is 3 V, the pulse width is 200 ps and the ambient background noise of the sound level meter is 55 dB. It can be seen that when the repetitive frequency is around 500MHz and 1GHz, the readings of the sound level meter peaks. Given a repetitive frequency of 500 MHz, the reading is higher than the background noise by about 10 dB; given a repetitive frequency of 1GHz, the reading is higher than the background noise by about 20 dB. When the repetitive frequency is fixed at 1 GHz, the quantitative influence of pulse width on the reading is shown in Fig. 4 (b). It can be observed that the influence of pulse width on the readings is almost negligible. Specifically, the readings remain unchanged when the pulse width is in the range 200 ~ 700ps. In the case of pulse width in 10 ~ 200ps, the readings are slightly influenced, and the possible reason is that the dipole radiation antenna's radiation efficiency is low. When the pulse width exceeds 800 ps, the coverage of pulse frequency is considerably narrowed, the number of frequency components that can interfere the sound level meter is reduced, and the readings begin to decrease gradually.

Effect Experiment

A prototype is designed for experiment on a recording pen, as shown in Fig. 5. Experimental steps are described as follows. The recording pen is first turned on to record the voice normally for about 10 s. Next, the prototype is initiated to interfere the pen for about 10 s. After that, the recorded contents are played to check whether the recording process is effectively jammed.

The horizontal directivity pattern of the beam radiated by the prototype is tested at a 6 dB beam angle of 98° in the microwave darkroom, as shown in Fig. 6. It can be seen that the recorded contents are nothing but noises that cannot be recognized. Hence, the prototype effectively jams the recording device.

The operation status of the recording device with and without interference from the prototype is quantitatively evaluated in Figs. 7 and 8. Specifically, Fig. 7 shows the waveform and spectrum of the normally recorded sound. The stored signal is digital and thus automatically regularized by the recording device. It can be seen from Fig. 7 (a) that the waveform has a peak of about 0.15, and its spectrum has a peak of 13.6 kHz, corresponding to a magnitude of -60dB. For the frequency below 8 kHz, its frequency spectrum range is approximately -90dB ~ -60dB. For the frequency 8kHz ~ 20kHz (exclusive of 13.6 kHz), the frequency spectrum range is below -90dB, as shown in Fig. 7 (b).

Figure 8 (a) indicates that the waveform of the recorded signal varies greatly after the recorder is jammed by the prototype. Due to the masking effect of the sound wave, the large-magnitude signal can effectively suppress the small-magnitude signal. One can find no normal sound signals from the recorded waveform; instead, there is only clattering noise whose peak is about 1.5 and larger than the normally recorded signal by 10 dB. This means that the sound is too suppressed to be restored. In Fig. 8 (b), the frequency spectrum magnitude of the jammed recording is larger than the normal recording by 10 dB. The spectral line at 13.6 kHz in Fig. 8 (b) is totally masked. Note that there are many types of recorders which vary greatly in terms of electromagnetic shielding and protection features. Hence, the interference performance of a jamming signal may vary considerably with the object it is applied to.

Conclusion

The principles on jamming the recorder using the mobile communication GSM signals are analyzed. Vulnerability of the recorder is discussed. The variation of the readings of sound level meter with the pulse width and repetitive frequency of the radiation signal is quantitatively measured, yielding insights into the setting of parameters for the jamming prototype. Experimental results demonstrate the ability of the prototype to effectively suppress the waveform of the recorded signal.

Acknowledgement

This paper is one of the research results of "The project of key protection technology of sensitive information leakage and theft in non-network environment in 2015".

References

[1] Neuber A, dickens J. “Electrical behavior of a simple helical flux compression generator for code benchmarking”. IEEE on Plasma Science, July 2001, pp. 1496-1455.

[2] Daniel K B, Tadeusz W. *Concept of an electromagnetic pulse laboratory*. Proc. Int. Symp in EMC, Wroclaw Poland, 1988.

[3] Adeleam N.T，Stavsky Y. “Flexual-Extensional Behavior of Composite Piezoelectric Circular Plates” Acoustics. 1980, pp. 819-825.