# The vehicle audio encryption system based on scrambling thought

Peibin Wu[1], Jindong Zhang[1,2, 3, a)], Yang Liu[1], Dongqi Han[1], Yiding Sun[1]

[1] *College of Computer Science and Technology, Jilin University, Changchun, 130012, China*
[2]*Key Laboratory of Symbol Computation and Knowledge Engineering of the Ministry of Education, Jilin University, Changchun,130012, China*
[3]*State Key Laboratory of Automobile Simulation and Control, Jilin University, Changchun 130025, China*

[a)] Corresponding author: zhangjindong_100@163. com

**Abstract.** In this paper, the vehicle audio encryption system based on scrambling thought and applied to vehicle-mounted media is proposed. The pseudo random number is generated each time it is encrypted, and it is substituted into the Fibonacci transform to generate a key with variable length. The audio data is divided by the number of pseudo random numbers into the Fibonacci sequence, and is encrypted in permutation encryption. The Fibonacci transform has symmetry and creates an audio file that cannot be parsed and played after the permutation encryption. In the security analysis of encryption algorithm, the audio files of different length are tested. The key space, anti-attack ability, key sensitivity and other indicators are tested to achieve good results. In addition, this algorithm is simple in calculation and can realize the ideal real-time performance in practical application.

**Key words:** vehicle media; audio encryption; scrambling thought; security analysis.

## INTRODUCTION

The rapid development of Internet of things technology and the frequent occurrence of information leakage events arouse the attention of intelligent product users and researchers on information security issues. With the development of research, the use of smart vehicles has gradually increased. Therefore, protecting the security of audio data on smart vehicles becomes a problem that cannot be ignored. Among them, the vehicle audio media not only needs to satisfy the basic security requirements of key encryption, but also has a good real-time performance.

To be specific, the research of audio encryption technology has been widely used, and there are many different implementations and application scenarios. Ashaswini, a. s., and d. Deepak, based on Z2's encryption algorithm, proposed Z4 system to generate pseudo-random number in the audio encryption application, making the algorithm more robust [1]. Lima, Juliano B., and Eronides F. da Silva Neto introduces an audio encryption scheme based on cosine transform (CNT), which is applied to the sample block of non-compressed digital audio signal recursively, which satisfies the main security requirements of key cryptography [2]. Liu, Hongjun, Abdurahman Kadir, and Yanling Li propose a lossless dual-channel audio encryption scheme based on one-time keys. the novelty is to apply chaotic system with changeable multi-scroll to generate keys, making brute-force attack impos-sible[3]. Nwe, Tin Zar, and Su Wai Phyo analyzed the performance of RSA and ElGamal algorithm based on execution time. According to the analysis results, the encryption and decryption time of RSA algorithm is much faster than that of ElGamal algorithm [4,5].

This paper designs an audio encryption technique based on scrambling thought. The pseudo random number is generated when the system is applied, and the key array is generated by the fibonacci transformation. And according to the pseudo random number into the fibonacci sequence to get the audio file division, scrambling encryption. The advantage is that the key space is large, and when applied to the on-vehicle media, this algorithm can not only resist the common cryptographic attacks, but also guarantee the good real-time performance.

## SYSTEM DESCRIPTION

In order to solve the problem of vehicle audio data security proposed in part one, this paper designs an audio encryption system based on scrambling thought. The flow chart of the encryption system is as follows:

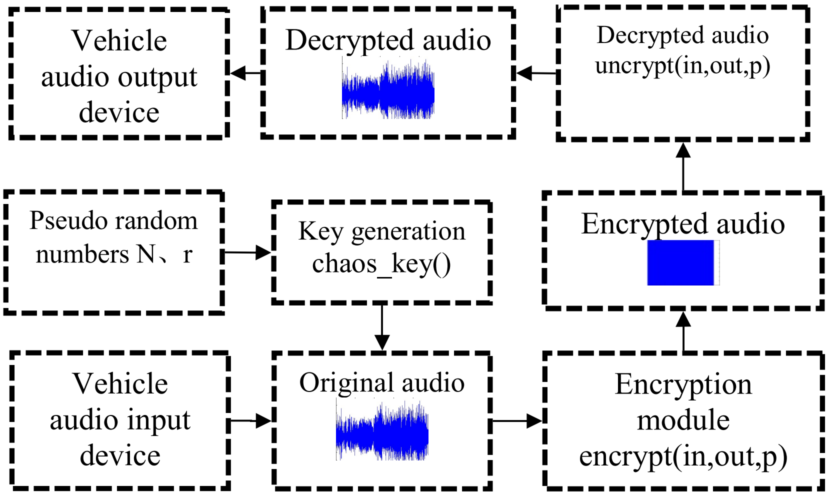
Vehicle audio output device
Decrypted audio
Decrypted audio uncrypt(in,out,p)
Pseudo random numbers N、r
Key generation chaos_key()
Encrypted audio
Vehicle audio input device
Original audio
Encryption module encrypt(in,out,p)

**FIGURE 1.** System flow chart

Fig.1 shows the flow of the encryption system. First, the original audio is inputted vehicle voice device. And then, when generating the key, two pseudo random numbers, r and N, will be generated first for the fibonacci transformation to generate the corresponding key array. The original audio data is scrambled and encrypted using this key to obtain an unplayable audio file. Decryption of the encrypted audio using the same key can get a decrypted audio file that is the same to the original audio data. In the implementation and testing of the algorithm, the first eight bits of the fibonacci sequence were tested for the convenience of the experiment. That is, the parameter K is 8, which can be changed according to the situation in practice. At last, in the listening end, through decoding, the vehicle audio player outputs audio.

## RESULTS AND ANALYSIS

The experimental environment is the operating system of win8.1. CPU is INTEL I5. Memory is 4GB, and hard disk is 500GB. The encryption algorithm was implemented using QT creator4.2.1 and the experiment was analyzed using Matlab R2013a. Anti-attack capability is a direct reflection of the effectiveness of encryption algorithms. In the test, a total of eight audio files were tested, with the audio one as an example to illustrate the effect of encryption. Fig.2&3 show the frequency domain diagram and the time domain diagram of 4037 KB original audio data.

The audio data in Fig.2&3 is encrypted by the encryption system described in part 2, and the encrypted audio file shown in Fig.4&5 are obtained. The encrypted audio files cannot be played. Fig.4 shows that the encrypted audio file has no regularities of distribution of original audio data. It can be seen from Fig.5 that the amplitude of the encrypted audio data is stable, without the residual of the original audio data.

Fig.6&7 are obtained by deciphering the encrypted audio file and analyze it. Comparing Fig.2&3 with Fig.6&7, the audio data after decryption is the same as the original audio data. The audio encryption system realizes lossless encryption and decryption of the audio file.

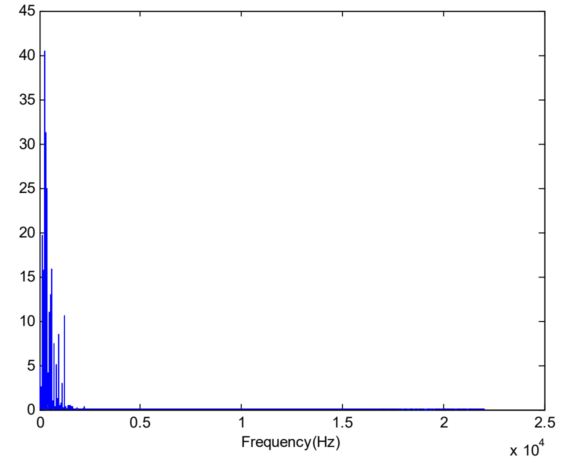

**FIGURE 2.** The frequency domain diagram of original audio

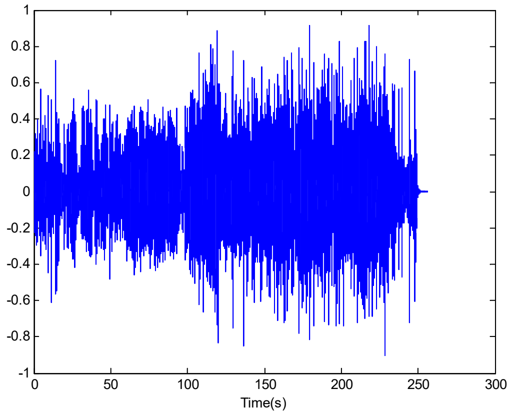

**FIGURE 3.** The time domain diagram of original audio

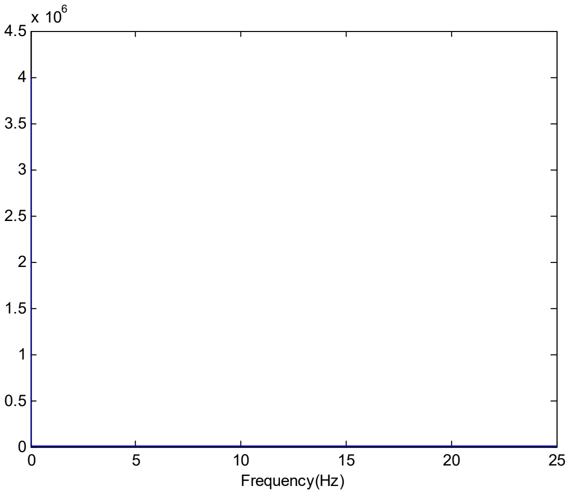

**FIGURE 4.** The frequency domain diagram of encrypted audio

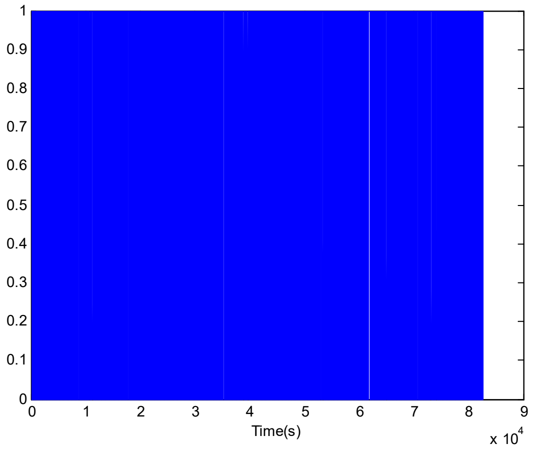

**FIGURE 5.** The time domain diagram of encrypted audio

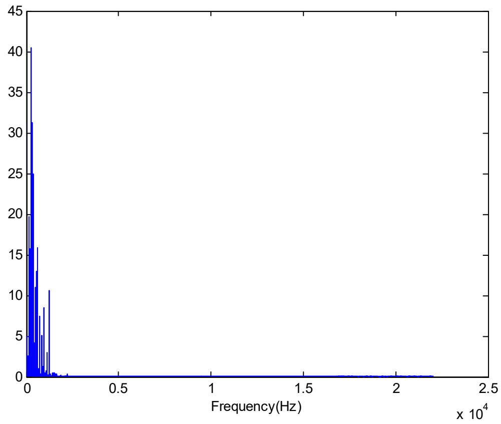

**FIGURE 6.** The frequency domain diagram of decrypted audio

The key space needs to be large enough to resist large-scale brute-force attacks. In this system, it can be seen from the second part that the key space gradually increases with the increase of variable k and the increase of the range limit of pseudo-random number r. Because the fibonacci sequence is an infinite series, as long as the computing power is sufficient, an infinite number of key combinations can be generated.

When scrambling encryption, the packet size is variable, increasing the difficulty of attack cracking. When the encrypted data is decrypted, a slight change in the key can lead to different results in the decryption process. In security encryption, small changes in the key must prevent attacks. For this scrambled encryption system, a small change in the key will result in the encrypted file being unable to be decrypted. As shown in Fig.8&9, when one bit of the key is changed, the encrypted audio cannot be decrypted and cannot be played.

The cost of performance and implementation is also an important concern for all practical applications. The best cryptographic algorithm is the one that strikes a good balance between security and performance. For the vehicle audio encryption system, in addition to the need to ensure data security, against third-party attacks, but also have a faster encryption and decryption speed, to prevent the pause during actual use.

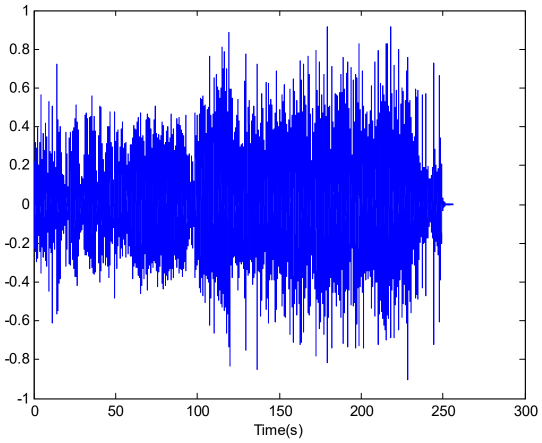

**FIGURE 7.** The time domain diagram of decrypted audio

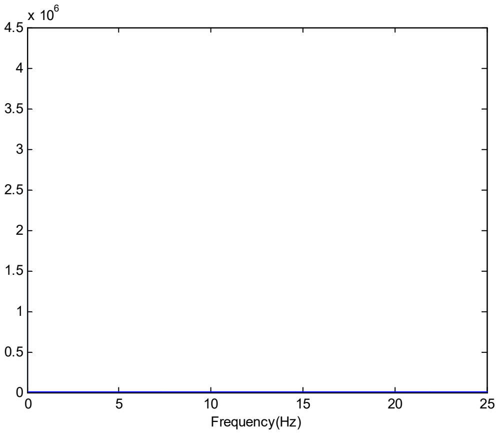

**FIGURE 8.** The frequency domain diagram of decrypted audio when there is a slight change in the key

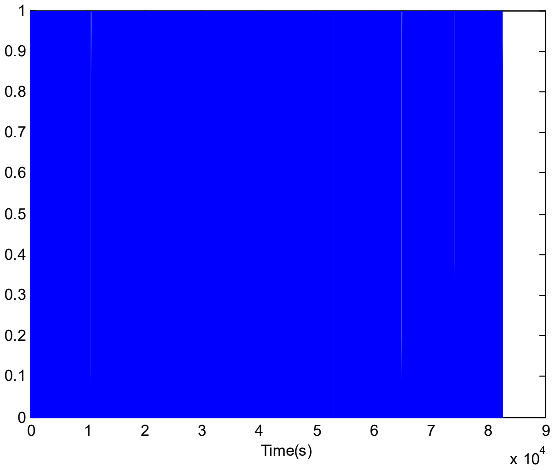

**FIGURE 9.** The time domain diagram of decrypted audio when there is a slight change in the key

## CONCLUSION

This paper proposes a vehicle audio encryption system based on the idea of scrambling. It combines the fibonacci sequence and generates a pseudo-random number to generate a key array. The audio file is divided into variable packet sizes for scrambling encryption. When a small change occurs in the key, the encrypted audio will not be cracked. The algorithm is simple in calculation, fast in running time and good in real time in practical application.

## ACKNOWLEDGEMENTS

This work is supported in part by the National Key Research and Development Program of China (2017YFB0102500), Natural Science Foundation of Jilin province (20170101133JC), and Jilin University (5157050847, 2017XYB252, 2017A53216).

## REFERENCES

1. Ashaswini A S, Deepak D. A Fast Audio Encryption Based Random Sequences Generated Using Linear Feedback Shift Register Defined Over Z4[J]. International Journal of Innovations & Advancement in Computer Science,2014,3(3),2347-8616
2. Lima J B, da Silva Neto E F. Audio encryption based on the cosine number transform[J]. Multimedia Tools and Applications, 2016, 75(14): 8403-8418.
3. Liu H, Kadir A, Li Y. Audio encryption scheme by confusion and diffusion based on multi-scroll chaotic system and one-time keys[J]. Optik-International Journal for Light and Electron Optics, 2016, 127(19): 7431-7438.
4. Nwe T Z, Phyo S W. Performance Analysis of RSA and ElGamal for Audio Security[J]. International Journal of Scientific Engineering and Technology Research, 2014, 3(11): 2494-2498.
5. Gunjan Gupta. Review on Encryption Ciphers of Cryptography in Network Security[J]. International Journal of Advanced Research in Computer Science and Software Engineering, 2012, 2(7):211-213.