A SYSTEM FOR DIGITIZING ANALOG SIGNALS, COMPRESSION AND ENCRYPTION

Dilyana Dimitrova*

* Department of Information Technologies, Nikola Vaptsarov Naval Academy

73 Vasil Drumev Str., Varna, Bulgaria.

E-mail: di.dimitrova@naval-acad.bg

(Selected from CEMA'24 Conference)

Abstract

This paper investigates the digitization, compression and encryption of analog signals. Digitization transforms analog signals into discrete digital form, crucial for efficient data processing and transmission in diverse industries. A-law compression is used to optimize the dynamic range of the signals by reducing the data needed to represent them while maintaining acceptable quality. Results demonstrate analog-to-digital conversion of sinusoidal signal and voice using an 8-bit ADC, confirming minimal signal loss with higher quantization levels. AES encryption is used to secure the digitized and compressed signal, ensuring data privacy. Future research will explore signal recovery methods and automated encryption techniques using Simulink. This study underscores the importance of digitization and encryption technologies in advancing communication systems reliability and security.

Keywords: ADC, AES, cryptography, digitization, encryption, signals, voice.

1. INTRODUCTION

In today's rapidly evolving world, the digitization of signals and voice plays a central role in numerous aspects of our everyday life. Digitization refers to the process of converting analog signals, which are continuous and variable, into digital ones, which are discrete and binary. This transformation is crucial for many reasons, spanning from enhanced data processing capabilities to improved storage and transmission efficiency.

In an era where the Internet of Things (IoT) is becoming widespread, the seamless connectivity between smart devices, sensors, and control systems is made possible through digital communication. This connectivity enables real-time monitoring, data analysis, and automation, driving efficiency and innovation across industries such as healthcare, transportation, and manufacturing.

Digital signals can be easily compressed, encrypted, and stored, offering significant advantages in terms of data management and security. Techniques like A-law compression, commonly used in Europe, allow efficient use of bandwidth and storage space. Encryption ensures that digital information can be transmitted securely, protecting sensitive data from unauthorized access and cyber threats.

In the field of voice communication, digitization has transformed how people interact and communicate. From mobile phones to VoIP (Voice over Internet Protocol) services, the conversion of voice to digital signal has enabled clearer, more reliable, and more adaptable communication methods. Features such as voicemail, and video calls have become standard, enhancing personal and professional communication.

Different studies have been made in this field. In paper [1] authors propose an encryption technology for voice transmission in mobile networks using the 3DES-ECC algorithm. It combines speech signal acquisition, 3DES, and ECC algorithms for speech data encryption. In [2] is presented speech to text conversion system that also encrypts the text using the Advanced Encryption Standard (AES) algorithm. In [3] authors introduce a k-shuffle based audio scrambling technique that produces cipher audio with variable audibility, beneficial for perceptual video encryption algorithms, showing resistance to certain types of attacks.

The absence of an analog-to-digital converter (ADC) that uses A-law compression and encryption of the signal following the literature review underscores the relevance of the issue.

The models in this paper present source digitization and A-law compression. A possibility for signal encryption is provided. For this purpose, two examples of digitization are examined – a sinusoidal signal, to clearly observe the signal transformation, and voice. The analog-to-digital converter is a fundamental block that enables the conversion of information from analog to digital form and its transmission to digital devices. Without analog-to-digital conversion, the world today would be very different. An A-law compression is selected because it is used in Europe.

The main aim of the paper is to explore and demonstrate the processes of analog-to-digital conversion and A-law compression in the context of digitizing signals, specifically sinusoidal signals and voice. Additionally, the paper highlights the significance of these processes in enhancing signal quality, reducing noise, and improving the efficiency of digital signal transmission. The study also investigates the application of encryption techniques, particularly using symmetric cryptographic algorithms like AES, to secure the digitized and compressed signals.

2. SOURCE DIGITIZATION

2.1. Components of the block diagram

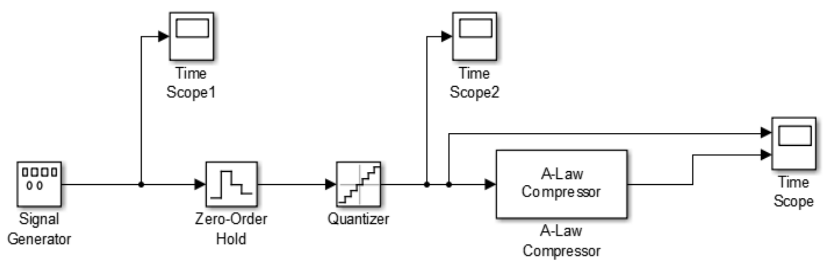

Figure 1. Block diagram of an ADC with A-law signal compression.

Figure 1 presents a block diagram of analog-to-digital conversion with A-law signal compression made in Simulink. The following blocks are used:

- Signal Generator - used to generate a sinusoidal signal.
- Zero-Order Hold - this block samples the signal at specific time intervals, Δt.

According to the Kotelnikov-Nyquist theorem [4], if there is a signal with a frequency band from f_{min} to f_{max} and take the reciprocal of the doubled maximum value of the frequency band, the time interval Δt should be less than or equal to this value to transmit it accurately to the receiver without distortion. This can be presented with formula (1).

$$\Delta t \leq \frac{1}{2f_{max}} \quad (1)$$

- Quantizer - discretizes the signal by amplitude and rounds it to the nearest allowed level. Rounding to an integer leads to distortion of the original signal and errors at the receiving end. There is a quantization step between two allowed levels, which is uneven, and the quantization is even.

- A-law Compressor - it uses an algorithm to compresses the signal's dynamic range and improves its quality.
- Several oscilloscopes that visually display the analog-to-digital conversion process.

2.2. Results from the source digitization simulation

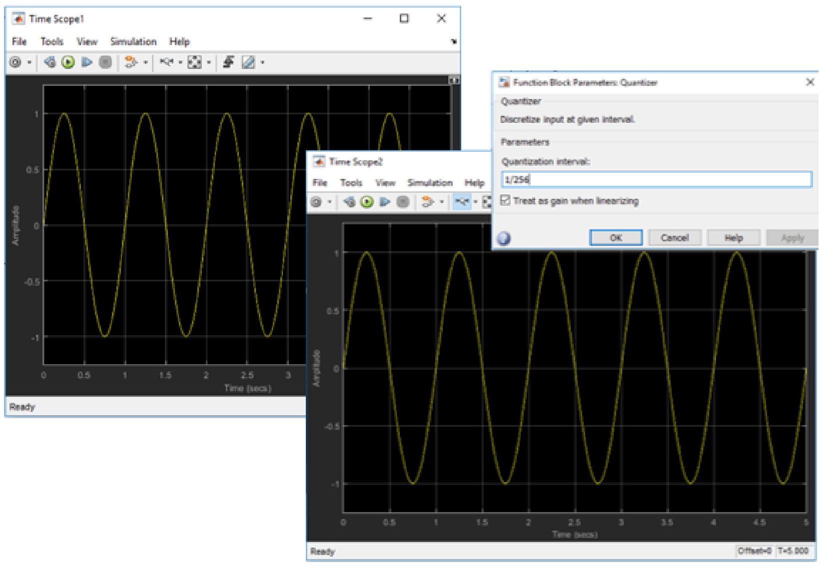

Figure 2. Graph of the analog signal from oscilloscope "Time Scope1" and the digital signal from "Time Scope2" with a quantization interval of 1/256.

According to ITU-T standard G.711 for pulse-code modulation (PCM) of speech frequencies [5], the best signal digitization is achieved using 256 quantization levels because it uses 8 bits for encoding speech. Therefore, the quantization interval in this case is equal to 1/256. After examining the oscilloscope graphs with this value, it was found that there is no visual difference between the analog and digital signals, as it is shown on Fig. 2, indicating that the conversion was performed with almost no loss.

To clearly observe the conversion of the analog signal to digital, and after testing different values that are powers of two, a noticeable difference in the graph without zooming in was seen at a quantization interval value of 1/32.

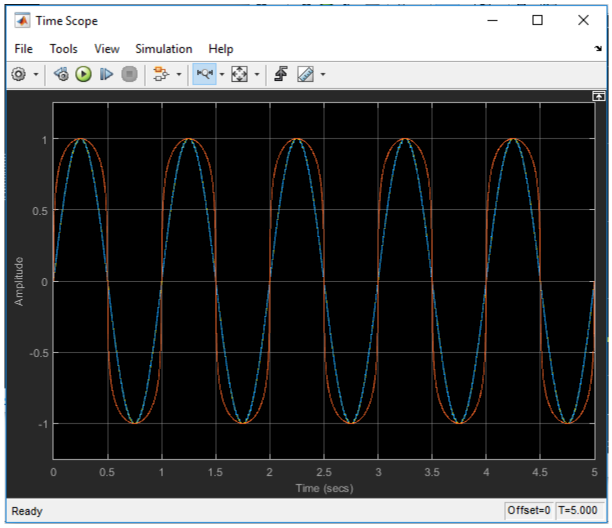

Figure 3. Graph from the “Time Scope” oscilloscope of the signal before and after analog-to-digital conversion and after A-law compression.

In Fig. 3, the analog signal and the digital signal are overlaid, and the A-law compressed signal, shown in red, clearly demonstrates that the quantization interval is non-uniform for the latter. The purpose of the compression is to improve the quality of the transmitted signal. In conclusion of the experiment, lower levels are more probable and carry more information, so they are quantized with a smaller step. The opposite is true for higher levels, so they are quantized with a larger step.

3. DIGITIZATION OF VOICE

3.1. Components of the block diagram

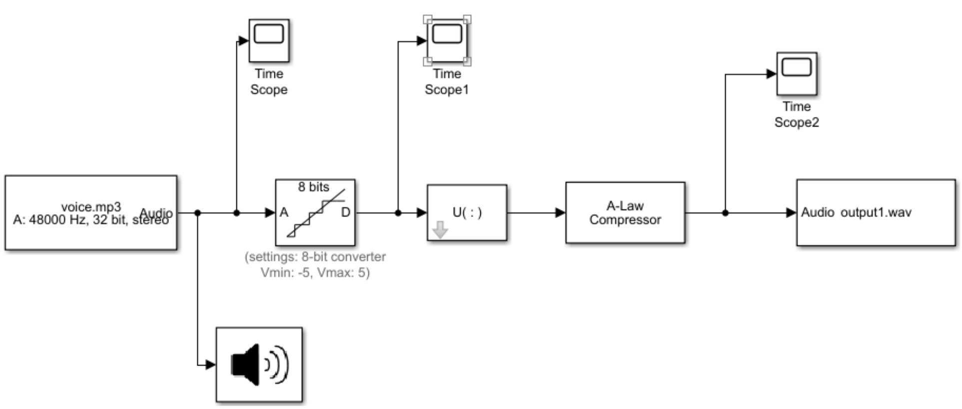

Figure 4. Block diagram of voice digitization.

In Fig. 4, a block diagram of voice digitization is presented. Its purpose is to demonstrate how speech is converted from analog to digital form and what happens to the signal after A-law compression. The following elements are used:

- Block that loads an audio file (From Multimedia file) - the file contains the author’s voice in m4a format or MPEG audio encoding. The signal is dual-channel since it is stereo and is recorded using phone's built-in microphone.
- Analog-to-Digital Converter (Idealized ADC quantizer) - used to convert voice signals, as using individual components for analog-to-digital conversion from the first diagram significantly increases the simulation time. In accordance with ITU-T standard G.711 for pulse-code modulation (PCM) of speech frequencies [5], an 8-bit ADC is utilized.
- Block for converting 2-D signal to 1-D - converts the two-dimensional stereo signal into a one-dimensional format, as the A-law compression block requires a one-dimensional input signal.
- A-law Compressor - the same as the one in first experiment.
- “To Audio Device” block - used for playback of the audio file.
- Oscilloscopes - used for graphical visualization of analog-to-digital conversion and A-law compression.

3.2. Results from the voice digitization simulation

In Fig. 5, two graphs illustrate the digital signal of the voice after processing by the ADC and a magnified view of it. These clearly show the analog-to-digital conversion. The signal is in two colors because it is dual-channel.

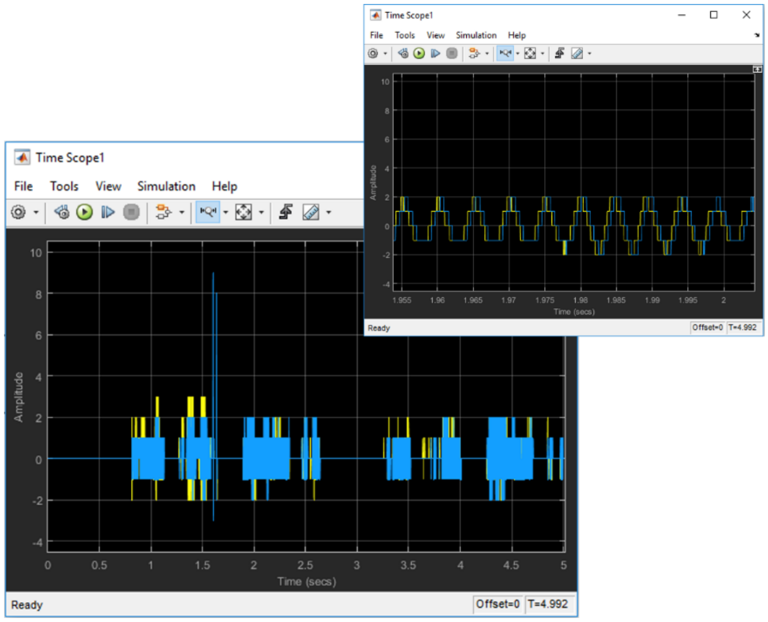

Figure 5. Graphs of the digitized signal (voice) from the “Time Scope1” oscilloscope.

Fig. 6 presents graphs of the signal after A-law compression. The wide dynamic range of speech is not well encoded by standard ADCs and their linear coding, as the quantization step is the same, leading to errors during analog signal reconstruction. For this purpose, A-law compression is used, where low frequencies are quantized with a smaller step and high frequencies - with a larger one, reducing the dynamic range of speech, minimizing quantization noise, and enhancing the quality of the transmitted digital signal.

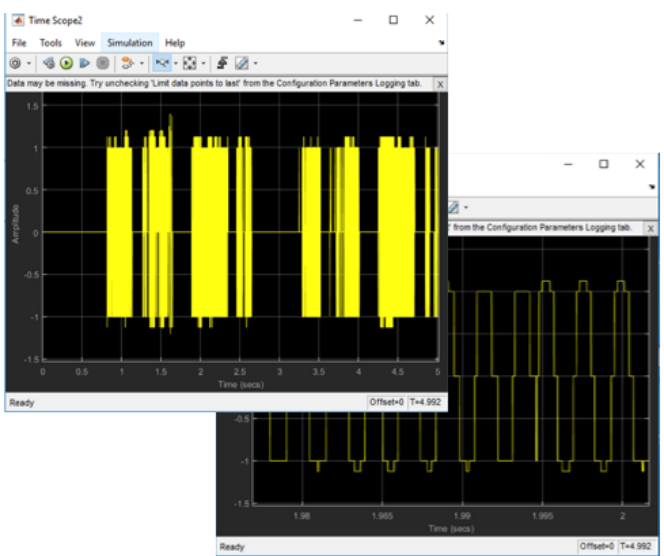

Figure 6. Graphs of the signal after A-law compression from “Time Scope2” oscilloscope.

4. ENCRYPTION

For encrypting the digitized and compressed signal, various cryptographic algorithms can be used. Symmetric cryptographic algorithms like AES are recommended for encryption of large volumes of information. During the experiment, AES encryption algorithm is utilized.

There are several approaches that can be implemented for encrypting the digitized and compressed signal. In this specific solution, the compressed signal is first saved into a WAV file using the built-in Simulink block "To Multimedia File". Subsequently, a MATLAB function is created to convert it into a binary file. The binary file is then encrypted with AES using external software. The decryption and information recovery processes were successful. As this paper is focused on digitizing the source signal, recovering the signal at the receiver will be a subject of future work.

Another potential approach for encrypting the digitized and compressed signal involves creating a Simulink function that automates the described procedures, which also remains a subject for future investigation.

5. CONCLUSION

During the study, graphical analog-to-digital conversion and A-law compression of sinusoidal signal and speech were observed. A possibility for signal encryption is provided. It was found that using higher levels of quantization provides better digitization of the analog signal. In the first case, 32 levels were used to observe the digitization process more closely. Comparing this with 256-level quantization, the digital signal showed no visible difference from the analog signal on the graph, indicating minimal loss during inverse conversion. In the second scheme, voice analog-to-digital conversion was performed using an 8-bit ADC according to G.711 standard, applying the same principles as in the first scheme. A-law compression was utilized in both cases to improve the quality of the transmitted digital signal. To secure the digitized and compressed signal, different cryptographic algorithms can be applied. Symmetric ciphers such as AES are preferred for their effectiveness with large data sets. In this experiment, AES was specifically utilized to encrypt the signal, providing strong security. Future research will explore signal recovery methods and automated encryption techniques using Simulink.

This study underscores the importance of digitization and encryption in advancing communication systems reliability and security.

The report is in implementation of the National Scientific Program "Security and Defense", adopted with RMS No. 731/21.10.2021, and financed by the Ministry of Education and Science of the Republic of Bulgaria according to Agreement No. D01-74/19.05.2022.

REFERENCES

[1] Chang, Z., Woźniak, M. Encryption technology of voice transmission in mobile network based on 3DES-ECC algorithm. Mobile Netw Appl 25, 2398–2408 (2020). https://doi.org/10.1007/s11036-020-01617-0
[1] Agarwal, A., Raj, P.M., & Katiyar, S. (2019). Secured Audio Encryption using AES Algorithm. International Journal of Computer Applications.
[2] Alhassan, S., Iddrisu, M.M. & Daabo, M.I. Securing audio data using K-shuffle technique. Multimed Tools Appl 78, 33985–33997 (2019). https://doi.org/10.1007/s11042-019-08151-6.
[3] V. V. Zamaruiev, "The use of Kotelnikov-Nyquist-Shannon sampling theorem for designing of digital control system for a power converter," 2017 IEEE First Ukraine Conference on Electrical and Computer Engineering (UKRCON), Kyiv, UKraine, 2017, pp. 522-527, doi: 10.1109/UKRCON.2017.8100305.
[4] International Telecommunication Union. "Recommendation G.711: Pulse Code Modulation (PCM) of Voice Frequencies." Accessed June 20, 2024. https://www.itu.int/rec/T-REC-G.711/.