Ministry of Education of the Republic of Belarus
Educational institution
Belarusian State University of Informatics and Radioelectronics

UDC 621.391.64

Dai Junyi

Software Module For Protection Of Information From a Leakage Via Acoustic Channels

Abstract to master degree thesis

Specialty 7-06-0611-02 Information Security

_____

Supervisor:
Zelmanski O.B., PhD, Associate Professor

_____

Minsk 2025

GENERAL DESCRIPTION OF WORK

The Research Aim and Objectives

The aim of the research is to analyze the existing methods for protecting information from leakage via acoustic channels and to develop an improved software tool that utilizes these findings to enhance acoustic privacy.

To achieve this aim, it is necessary to solve the following objectives:

1) to understand the basic ideas of acoustic channels and how they are used in everyday products.

2) to look at different eavesdropping methods, how they are grouped, and the risks of information leaks through acoustic channels.

3) to check how well physical soundproofing methods work to stop sound from escaping.

4) to study electronic ways to block eavesdropping, like sound masking and speech encryption, and how they help protect information.

5) to see how AI and machine learning can improve acoustic privacy by simulating sound in real time.

6) to create a software tool that uses API access to existing neural networks to generate random phrases that confuse eavesdroppers.

Work Connection with Priority Areas of Scientific Research

The topic of the thesis corresponds to paragraph 6 Ensuring the security of humans, society and the state (means of technical and cryptographic information protection, cryptology and cybersecurity) of the list of priority areas of scientific, scientific-technical and innovative activities for 2021–2025, approved by the Decree of the President of the Republic of Belarus dated 07.05. 2020 No. 156.

Thesis Results Approbation

The main results of the dissertation were reported and discussed at the 60th Scientific conference of Graduate Students, Master Students and Students of BSUIR (Minsk, April 22–26, 2024), international scientific and practical conference "Information Resources Management" (Minsk, March 29, 2024).

INTRODUCTION

Acoustic channel information leakage has become a significant concern in various fields, including economic activities, military operations, and security systems. The advantages of acoustic protection methods include their effectiveness, non-intrusiveness, and relatively low implementation costs, making them increasingly relevant in today's digital landscape. As companies become more aware of the risks of information theft through sound, the need for strong protective solutions is expected to grow. That's why studying ways to prevent acoustic data leaks is highly important. This paper focuses on three key areas: understanding how sound channels work, examining eavesdropping methods, and exploring ways to protect information. Specifically, we look at using existing neural networks through API to mimic user voices and create meaningless phrases to mislead potential eavesdroppers.

This paper centers on three main areas: understanding acoustic channels, analyzing eavesdropping technologies, and exploring countermeasures for information protection. In particular, we delve into the use of existing neural network models via API to simulate user voices, thereby producing meaningless phrases that confuse potential eavesdroppers. The primary objectives of this paper are:

– to analyze the basic principles of acoustic channels and their applications in everyday products;

– to evaluate various eavesdropping technologies and assess the risks of information leakage;

– to investigate physical and electronic countermeasures for protecting information from acoustic leakage;

– to explore the role of AI and machine learning in enhancing acoustic privacy;

– to implement a software tool that utilizes neural network models to generate confusing audio content in real-time;

– to conduct tests on the effectiveness of the proposed solution in various acoustic environments.

The developed software tool demonstrates a significant improvement in protecting information from acoustic leakage, effectively simulating user voices to obscure sensitive audio content.

MAIN PART

The first chapter provides a comprehensive overview of acoustic channel information leakage, detailing the basic principles of acoustic channels and their applications in everyday products. It emphasizes the significance of understanding eavesdropping technologies and the risks associated with information leakage [1–A.2–A].

The second chapter outlines the design and implementation of a software model aimed at protecting information from acoustic leaks. It discusses the system design goals and requirements, including various protection scenarios and core functional requirements. The chapter also presents the web application architecture, detailing the overall design, front-end, back-end, and database structures. Key highlights include the implementation of a voice clone module and an analysis of existing sound cloning technologies, along with the specific voice cloning technology used in the selected platform.

In the third chapter, the software model is deployed and accessed in various environments. It details server environment requirements and different methods for system access. Additionally, this chapter demonstrates the user operation process, including user authentication features and a guide to using core functions. The results indicate that the software tool successfully generates meaningless phrases in real time, effectively confusing potential eavesdroppers. This chapter concludes with an assessment of the system's performance, showcasing its ability to enhance acoustic privacy and protect sensitive information from unauthorized access.

CONCLUSION

This study aims at the acoustic channel information leakage problem faced by the current information security field, and designs and implements an acoustic channel information leakage prevention software model based on a Web application. With the popularization of smart devices, the risk of privacy leakage caused by continuous microphone monitoring is becoming increasingly prominent, especially in highly confidential places such as government agencies, military departments and enterprises, where the consequences of information leakage are particularly serious.

To solve this problem, this study proposes an innovative technical solution, which uses real-time audio processing technology to generate meaningless words similar to the user's voice, and plays them through a Web application to interfere with the monitoring device's recognition of the user's conversation content. The core of this technical solution lies in the cloning and analysis of the user's voice, as well as the realization of the function of real-time generation and playback of meaningless words.

The study results show that the software model can play a good role in preventing information leakage in various scenarios. In highly confidential meetings or calls, users can significantly reduce the risk of information leakage by running the software. In addition, the software is also highly practical and flexible, and can be applied to multiple fields such as personal privacy protection, corporate trade secrets protection, and national information security.

In summary, “Software Module For Protection Of Information From a Leakage Via Acoustic Channels” is not only innovative, but also has high practical value and application prospects, providing new ideas and technical means for the development of the information security field. In the future, the software model will continue to be optimized and improved to further improve its anti-information leakage effect and practicality.

LIST OF OWN PUBLICATIONS

1-A. Dai, Junyi. Speaker identification for speech information protection systems / K.P. Shakin, E.A. Makarenya, Dai Junyi // 60th scientific. conf. of postgraduates, master's students and students of the educational institution "Belarusian State University of Informatics and Radioelectronics": materials of the report. scientific. conf., Minsk, April 22-26, 2024 / BSUIR. - Minsk, 2024. - P. 21-23.

2-A. Dai, Junyi. Speaker identification as an element of the speech information protection system / E.A. Makarenya, K.P. Shakin, Dai Junyi // XX international scientific and practical conference "Information Resources Management": materials of the report. scientific. Conf., Minsk, March 29, 2024 / Academy of Public Administration under the President of the Republic of Belarus. - Minsk, 2024. - P. 318-321.