ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 5, Issue 1, July 2015

Security System for Sending Information Containing Hidden Voice Data by Steganography (SIOVE) Using Matlab

Bárbara Emma Sánchez Rinza, María del Rocío Guadalupe Morales Salgado*, Cristian Omar Cortez Olguín
Faculty of Computer Science, Benemérita Universidad Autónoma de Puebla, Universidad Popular Autónoma del Estado de Puebla Puebla, Puebla

Abstract*—with the modern use of technology and communication, data and information travel through many channels. During transmission they may be vulnerable to passive or active attacks, in which messages are used by criminal groups to undermine the integrity of individuals and institutions. In this study, a solution is proposed that uses a system constructed in MATLAB that is able to hide voice signals in an image. That is, the data sent is an image but it carries a protected voice message within it. This solution seeks to ensure the integrity of the data. To contextualize this work, the concepts of steganography and voice signals are defined. The implementation of the SIOVE system and its application are also presented

I. INTRODUCTION

Computer security consists of ensuring that an organization's computer resources are being utilized in the manner determined by the organization, and that data access and modification can only be carried out by authorized people and within the limits of their authorization.[1,2]
The main objectives of computer security are [3]:

- Detect potential problems and security threats, minimizing and managing risks.
- Ensure proper use of resources and application of systems.
- Limit losses and implement system recovery in the event of a security incident.
- Comply with the legal framework and with overall organizational requirements

A. Steganography

The word 'steganography' comes from the Greek words steganos (hidden) and graphos (writing), and can be defined as a technique for hiding information in a covert channel in order to prevent a hidden message from being detected. When a message is transmitted, someone spying on the communication transmission may not be able to decipher it, but they will at least know that an encrypted message has been sent, when it was sent, and how much encrypted data was exchanged. When this knowledge constitutes a threat to the organization, we can employ steganography [4]. As explained above, steganography consists of hiding a secret message inside another message that is not secret. The very existence of the secret message is concealed. If the steganographic message is also encrypted, we can keep its content secret even if its existence is detected upon transmission. It is easier to conceal a message in information that can be expressed with a variable amount of data, such as a photograph, audio or video. An example of steganography is hiding a message inside another message consisting of a hidden "signature" in a set of data. When an unauthorized copy is made of the data, the source can be detected by comparing characteristics such as size and existence of associated codes using the LSB (least significant bit) technique. No "watermark" algorithm has yet been found that is resistant to every possible data manipulation, such as the introduction of noise, changing image resolution, overwriting the signature, or other techniques. The elements or actors in steganography are [4, 5, 6]:

- Container: The object that is used to carry the hidden message.
- Stego-object: The container plus the concealed message.
- Adversary: Any of the entities from which the concealed information is being hidden.
- Steganalysis: The science of detecting (passive attacks) and/or rendering harmless (active attacks) information hidden in some sort of container, and of finding useful information within the container (existence and size).

In general terms, steganography is divided into two types [7, 8,9]:

- Linguistic steganography.
- Technical steganography.

Linguistic steganography uses a written text as the carrier, while technical steganography uses any other type of carrier, which may be audio, images, video, or other data. This paper deals with technical steganography [10].

B. Voice Signals

The voice is a signal that transmits conscious, intelligent information produced by humans in such a manner that listeners can obtain information directly without the need for any further source of information such as images or text.

For voice signals, the most efficient encoders use a speech production model consisting first of an excitation that models air flowing from the lungs and vibration of the vocal cords and secondly a filter that represents the oral and nasal cavity. Both voice and audio signals use a model of an auditory perception system that indicates which components of the signal do not have to be kept because they are not heard, as they are masked in both time and frequency by neighboring higher-energy components of the signal [12]. A spectral representation serves as a simple way to represent relevant

ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 5, Issue 1, July 2015

frequency characteristics of the voice signal. Figure 1 shows the spectrum of the signal corresponding to a generic loud voice. We can see features such as formants (local maxima in the spectrum), and the fundamental frequency (ripple) and its harmonics. The fundamental frequency is the frequency of vibration of the vocal cords, which determines the pitch.

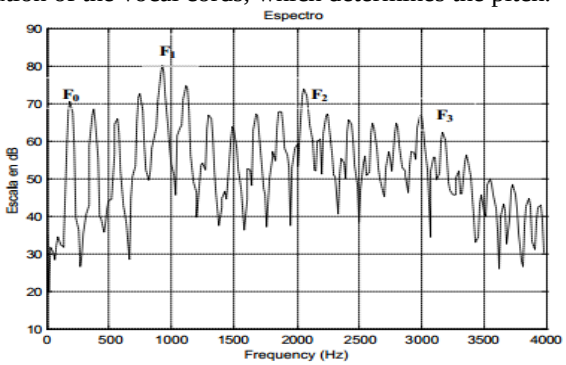

Fig 1. Spectrum of a generic speech signal.Source: Authors.

II. IMPLEMENTATION AND APPLICATION OF THE SIOVE SYSTEM

To implement the steganography process in information security, the LSB (least significant bit) technique is used. First the message to be concealed is decomposed in order to be able to insert it into the voice signal. The result is a visible message that carries a hidden message within it. As noted above, the program was written in MATLAB, since it has a friendly graphical interface and a wide variety of options [11]. Figure 2 shows the interface of the SIOVE system. It offers the functions of recording the audio to be sent and adding a message in text form to be hidden in the original message The two can then be merged for transmission as a single audio signal, preventing an intruder from being able to capture the text message [13,14].

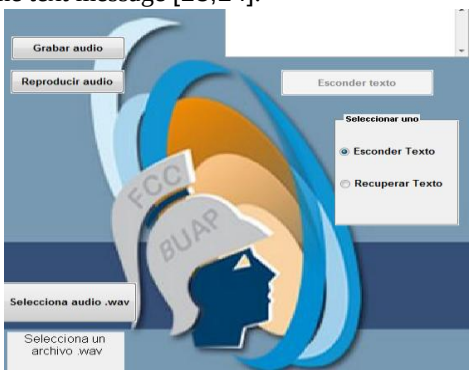

Fig 2. Graphical interface of the SIOVE program.Source: Authors.

The SIOVE program lets you record a voice signal and play back a previously recorded audio file. To use the program, a voice signal can either be recorded or an existing file selected with the "Select .wav file" button. After the audio file is chosen, the "Hide text" button becomes active. The user writes a message in the text field and clicks on "Hide text." As shown in Figure 3, the program saves the audio file with the *.wav extension.

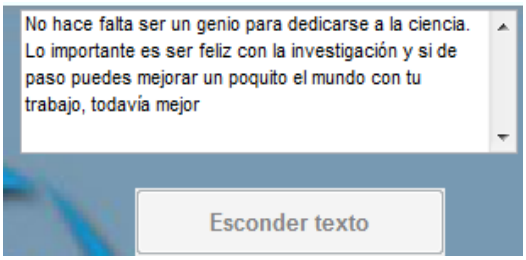

Fig 3. Message to be hidden. Source: Authors.

To retrieve the message, the "Recover text" option is selected. Another option offered by the system is that of checking whether an audio file contains hidden text or not. To do so, the user clicks "Select .wav file," and the program automatically shows the hidden message concealed in the audio file. If there is no hidden message, it displays a dialogue box with the message "The file does not contain hidden text." Figure 4 shows two messages hidden in different audio files.

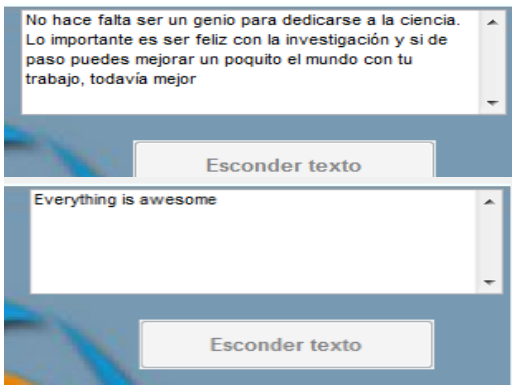

Fig 4. Concealed messages.Source: Authors.

In order to verify that the steganography technique was correctly applied, the original audio file and audio file with the hidden text were played. The two messages sounded exactly the same to the human ear although there was actually a hidden message inside one of them. Figure 5 shows the spectrum of an original audio signal and the same signal with a hidden message.

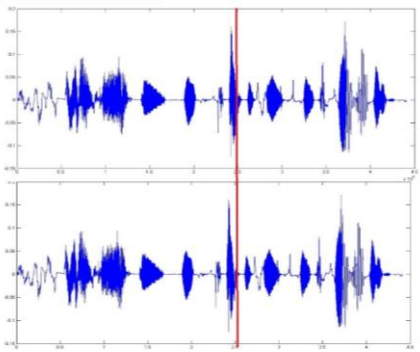

Fig 5. Original audio signal and audio with hidden message. Source: Authors.

III. CONCLUSION

This secure system for sending information concealed in voice signals by means of steganography (SIOVE) using MATLAB is a solution for the problem of communication attacks that can affect voice messages. Potential future work in this area could be to compare this with other methods and

ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 5, Issue 1, July 2015

algorithms such as cryptography to verify the efficiency and effectiveness of SIOVE. Future work that can be done is to improve the accuracy and also create an application for mobile devices.

REFERENCES

[1] Aceituno C. Vicente, Seguridad de la información, First edition, Editorial Limusa, Mexico, 2006. ISBN 968-18-6856-0.

[2] Pino C. Gil, Seguridad informática. Technical criptográfica, First edition. Editorial Alfaomega, Mexico, 1997. ISBN 970-15-0328-7.

[3] Cole E., Krutz, R., Conley J. W., Network Security Bible, Wiley, Indianapolis, IN, 2006. ISBN 0-7645-7397-7.

[4] Nestler V. J., Conklin W. A., White G. B., Hirsch M. P., Computer Security Lab Manual, McGraw-Hill/Irwin, NY, 2006. ISBN 0-07-225508-0.

[5] Gómez V. Álvaro, Enciclopedia de la seguridad informática, First edition, Editorial Alfaomega, Mexico, 2007. ISBN 978-970-15-1266-1. ISBN: 970-26-0316-1.

[6] Anderson R. and Petitcolas F., IEEE Journal on Selected Areas in Communications, "On the limits of steganography", 16(4): 474–481, 1988.

[7] Marvel L. M., Boncelet C. G., Retter C. T., IEEE Transactions on Image Processing, "Spread spectrum image steganography", 8(8):1075–83, 1999.

[8] Crandall R., "Some notes on Steganography", Steganography Mailing List, December 18, 1998.

[9] Sánchez Rinza Barbara E., Cano C. M., Avances de investigación aplicada en ciencias de la computación, "Steganography algorithm marb of carriers on charts." 2009. ISBN 9786074871234

[10] Johnson N. F., Jajodia S., "Exploring steganography: Seeing the unseen," IEEE Computer 31(2): 26–34, 1998.

[11] Schaathun G. H., "Basics of LSB and MATLAB," Spring 2008, University of Surrey.

[12] Olanrewaju R.F., Khalifa O., Rahman H.A., "Increasing the hiding capacity of low-bit encoding audio steganography using a novel embedding technique," World Applied Sciences Journal 21: 79–83, 2013, ISSN: 1818-4952

[13] Mazurczyk W., Szaga P., Szczypiorski K., "Using transcoding for hidden communication in IP telephony". 2014 doi:10.1007/s11042-012-1224-8

[14] Tomasi W., Sistemas de comunicaciones electrónicas, Fourth edition, Prentice-Hall., Mexico, 200.

AUTHOR'S PROFILE

Bárbara Emma Sánchez Rinza Bachelor in Physics, Master Degree in Optics, Doctor's Degree in Optics. She has written 42 chapters of books, 32 national and international paper, 12 memoirs. She has participated in 104 conferences in different forums. She has directed 27 Bachelor Thesis and 6 Master Thesis.