Computers and Electrical Engineering 68 (2018) 425–436

Contents lists available at ScienceDirect

Computers and Electrical Engineering

journal homepage: www.elsevier.com/locate/compeleceng

Covert communication model for speech signals based on an indirect and adaptive encryption technique☆

Haider Ismael Shahadi

Department of Electrical and Electronic Engineering, Faculty of Engineering, University of Kerbala, Karbala, 56001, Iraq

ARTICLE INFO

Keywords:
Multimedia security
Indirect encryption
Speech hiding
Speech encryption
Wavelet transform
Covert communications

ABSTRACT

This study proposes an indirect speech encryption technique that applies the chameleon style. A chameleon adapts its skin colour according to its surrounding environment to protect itself from its enemies. The proposed model adapts the wavelet coefficients of a secret speech to any other speech signal coefficients to make them similar. Subsequently, the vector to the adaptation that involves the original positions of the secret speech samples is sent to the receiver instead of the encrypted message or cover speech. The proposed method does not send the encrypted contents of the secret speech (such as that in traditional encryption) nor extends the bandwidth of the transmitted messages (such as that in a steganographic system). The proposed technique has been tested on several speech signals, and the reconstructed speeches have produced sounds that are similar to the original speeches with a normalised correlation of over 95%. Moreover, the model is robust against plaintext and ciphertext attackers. The proposed technique can be used in applications that require high-level security, such as military and intelligence communications.

1. Introduction

The rapid development of digital communications has made information security a critical issue in industries, businesses and governments. Modern cryptography and steganography have recently produced essential techniques for information security and data protection [1,2]. Encryption modifies a secret message to make it incomprehensible to illegal receivers. By contrast, steganography hides a secret message in a host medium to make it unnoticeable to illegal receivers [1,3,4].

In the literature, numerous methods have been proposed to encrypt speech signals. Some of these methods use standard data encryption algorithms, such as the techniques presented in [5–8]. In [5], the authors applied the blowfish algorithm based on a conjugate structure algebraic coding technique. This scheme modifies the method for generating substitution boxes to reduce time complexity. In [6], the author implemented the hardware of the Rivest–Shamir–Adleman (RSA) algorithm. Moreover, wavelet decomposition was used to compress data and minimise the quantisation noise level of perpetual audio masking. In [7], a hardware implementation of the Data Encryption Standard (DES) scrambler was achieved using field-programmable gate array. In [8], the authors evaluated the effect of the Advanced Encryption Standard (AES) encryption algorithm on Voice over Internet Protocol (VoIP) systems. Another group of speech encryption methods are based on chaotic algorithms and Pseudo-random number generators, such as those presented in [9–12]. Other speech encryption methods are based on blind source separation, such as those proposed in [13,14].

Alternatively, digital steganography is used as a security technique that does not raise or attract suspicion to secret data. Several steganographic approaches have been proposed to hide speech signals. Some of these approaches hide a secret speech in the least

☆ Reviews processed and recommended for publication to the Editor-in-Chief by Area Editor Dr. E. Cabal-Yepez.
E-mail address: haider_almayaly@uokerbala.edu.iq.

https://doi.org/10.1016/j.compeleceng.2018.04.018
Received 22 December 2017; Received in revised form 23 April 2018; Accepted 24 April 2018

significant bits of coefficients in a transform domain, such as discrete cosine transform [15], discrete Fourier transform [16] and discrete wavelet transform (DWT) [2,17,18].

Encryption and steganography techniques have their respective drawbacks. Encrypted messages raise suspicions and attract the attention of hackers and attackers [5–8], whereas hidden messages in cover media require considerably higher storage or bandwidth than encrypted messages to save or transmit stego data. Therefore, the current study proposes an indirect encryption technique for speech signals to send data without raising suspicions and that does not require additional bandwidth. The proposed technique considers the human auditory system (HAS) in its hypothesis.

The rest of this paper is organised as follows. Section 2 presents the hypothesis and formulation used in the proposed method. Section 3 explains the proposed indirect encryption method. Section 4 presents the test results of the proposed method and provides a discussion. Section 4 gives a comparison with other works. Finally, Section 5 concludes the study.

2. Wavelet coefficient adaptation (WCA)

One example of natural adaptation is demonstrated by a chameleon, which adapts its skin colour to its surrounding environment to become undetectable to its enemies. In a similar manner, we can make a secret speech undetectable by adapting it to another speech. The primary objective of any security model is to make secret messages undetectable. The proposed model is inspired by the adaptation behaviour of a chameleon. Accordingly, the proposed hypothesis states that ‘any secret speech can appear similar to another speech if their coefficients in the wavelet domain are organised according to their coefficient amplitudes’. Therefore, the proposed method changes a secret speech signal to make it similar to any other speech signal by varying the positions of its wavelet coefficients. The methodology steps of the hypothesis are described as follows.

Suppose that two speech signals correspond to two different speakers: speech$_1$ and speech$_2$. Speech$_1$ is related to the cover speech ($CS[n]$), whereas speech$_2$ is related to the secret speech ($SS[n]$). In this study, the cover speech refers to a carrier signal in steganography and to a secret key in cryptography. The steps of WCA are described as follows.

Step 1: $CS[n]$ and $SS[n]$ are decomposed using a DWT-based Haar filter to obtain their wavelet coefficients. The transformation is denoted by

$$\begin{aligned} &CS[n]\overrightarrow{\ DWT\ }\ CS[w] \\ &SS[n]\overrightarrow{\ DWT\ }\ SS[w] \end{aligned} \tag{1}$$

where $CS[w]$ and $SS[w]$ are the wavelet coefficients of the cover and secret speeches, respectively.

Step 2: The wavelet coefficients can be set to zero because they have low amplitudes and do not provide significant energy to the signal. This process is known as thresholding, which is optional process in WCA. Hard thresholding is applied according to the following:

$$\widetilde{S}(w) = \begin{cases} S(w) & |S(w)| \geq thr \\ 0 & |S(w)| < thr \end{cases}, \tag{2}$$

where thr denotes the threshold, and $\widetilde{S}(w)$ denotes the wavelet coefficient after thresholding. $\widetilde{CS}(w)$ and $\widetilde{SS}(w)$ are estimated at the output.

Step 3: $\widetilde{CS}(w)$ and $\widetilde{SS}(w)$ are arranged in descending order and denoted as follows:

$$\begin{aligned} &\widetilde{CS}[w]\overrightarrow{\ Sorting\ }\ \widetilde{CS}_s[w] \\ &\widetilde{SS}[w]\overrightarrow{\ Sorting\ }\ \widetilde{SS}_s[w] \end{aligned} \tag{3}$$

where $\widetilde{CS}_s[w]$ and $\widetilde{SS}_s[w]$ are the sorted coefficients of the cover and secret speeches, respectively. The original positions of the wavelet coefficients for the $\widetilde{CS}_s[w]$ and $\widetilde{SS}_s[w]$ matrices are saved in vectors J_{CS} and J_{SS}, respectively. Subsequently, three regions are clearly distinguished in each $\widetilde{CS}_s[w]$ and $\widetilde{SS}_s[w]$. These regions are the positive coefficients (left), null coefficients (middle) and negative coefficients (right). The sorted wavelet coefficients will constantly exhibit this behaviour regardless of the selected speech signals. Fig. 1 illustrates an example of the sorted wavelet coefficients of two speech signals; the signals have the same number of samples. Each speech signal coefficient of the three regions is clearly shown in the figure.

Step 4: This step involves reordering the coefficients of $\widetilde{SS}_s[w]$ (the secret speech). That is, its wavelet representation will be similar to that of the cover signal ($\widetilde{CS}_s[w]$). Subsequently, the first coefficients of $\widetilde{SS}_s[w]$ are located in the first positions found in