Resumen de Tesis Doctoral

UNIVERSITAT POLITÈCNICA DE CATALUNYA
BARCELONATECH
Escola de Doctorat

DNI/NIE/Pasaporte	Y1404451Q
Nombre y apellidos	Dora Maria Ballesteros Larrotta
Título de la tesis	Methods of covert communication of speech signals based on a bio-inspired principle
Unidad estructural	Doctorado
Programa	Doctorado en ingenieria electroncia
Códigos UNESCO	332902 | 120326 | 120714 |

(Mínimo 1 y màximo 4, podéis verlos en
http://doctorat.upc.edu/gestion-academica/carpeta-impresos/tesis-matricula-y-deposito/codigos-unesco)

Resumen de la tesis de 4000 caracteres máximo (si se superan los 4000 se cortará automáticamente)

This work presents two speech hiding methods based on a bio-inspired concept known as the “ability of adaptation of speech signals”. Suppose there are two speech signals, the first one is the secret message and the second is the target speech signal which has non-sensitive information, therefore the secret message can be manipulated so it resembles the target speech signal.

The ability of adaptation of speech signals is used to scramble speech signals in wavelet domain. Unlike traditional approaches, the scrambled speech signal is a legible speech signal and the permutation process is based on the adaptation between the secret's coefficients and the target' coefficients. Then, the system can be viewed as a special case of Time-Frequency Scrambling (TFS). It works with perfect secrecy because the key-space length is equal to the secret-space length, there are as many secret messages as scrambled speech signals, and the mapping between inputs and outputs is one-to-one. It is concluded that the system overcomes the brute force attack. Additionally, the secret message can be recovered by the intended user even if the scrambled speech signal is attacked by compression, re-sampling or filtering attacks.

In the case of steganography, two schemes were proposed. The first one is known as Efficient Wavelet Masking (EWM) and the second one as improved Efficient Wavelet Masking (iEWM). They take advantage of the masking property of the Human Auditory System (HAS) by using an efficient process of masking based on the adaptation of the secret message to the host signal. The first one, EWM, uses an indirect LSB substitution based on a parameter, Pd, which relates the amplitude of the host signal with the amplitude of the adapted-speech signal. The 5-LSBs of the host’s coefficients are replaced with the parameter Pd. Unlike EWM, iEWM uses direct LSB substitution. In this case, the adapted-secret message is directly hidden into the host signal, in wavelet domain. The number of bits varies according to the amplitude of the host’s coefficients and therefore, the higher the amplitude, the higher is the number of replaced bits. Nevertheless, the MSBs of the host’s coefficients are kept and it is controlled with the parameter Significant-Bit-to-Hold (SBH). While EWM is highly transparent (it means that the stego signal does not generate suspicious about the existence of the secret message), iEWM is highly robust against signal manipulations attacks.

Since both the proposed steganography scheme and the scrambling scheme require knowing in advance the secret message and the target (host) speech signal, they are not suitable for real-time operation. Therefore, it is presented a scheme which works on hardware devices and the stego signal is quasi-immediately generated as the secret message is pronounced.

Lugar	Barcelona, España	Fecha	26/04/2013

Firma