

Resumo da Dissertação apresentada à UFPE como parte dos requisitos necessários para obtenção do grau de Mestre em Engenharia Elétrica.

**Implementação de um Sistema Esteganográfico para  
Inserção de textos em Sinais de Áudio**

**Jinnett Pamela Carrión Casiera**

Março/2009

Orientadores: Hélio Magalhães de Oliveira, Ricardo Menezes Campello de Souza

Área de Concentração: Comunicações / Processamento de Sinais

Palavras-chave: Ocultação de Informação, Esteganografia, Dados, Sinais de Áudio, *Wavelet*.

Número de Páginas: 152 <http://repositorio.ufpe.br:8080/xmlui/handle/123456789/5409>

A arte de ocultar uma mensagem dentro de outro objeto é conhecida como esteganografia, na qual o objetivo principal é que a mensagem oculta não seja percebida. Uma rápida análise na história da esteganografia conduz naturalmente a visualizar seu desenvolvimento, desde os primitivos métodos manuais até as aplicações digitais atuais. O desenvolvimento da tecnologia tornou factível a aparição de modelos esteganográficos que exploram as características e fraquezas de arquivos digitais. Detalham-se técnicas convencionais para ocultação de mensagens, assim como a abordagem do método desenvolvido. Este novo método de esteganografia em dois passos combina a cifragem do texto-pleno através de um criptosistema padrão, seguido pela imersão dos dados cifrados no arquivo de áudio. O trabalho enfoca-se na inserção de textos curtos em arquivos com formato wav – a entrada dos dados é realizada nas componentes que resultam da transformação do sinal mediante as transformadas de *wavelet*, empregando uma técnica que insere a informação de texto nas três primeiras casas decimais dos coeficientes da transformada, restringindo o tamanho da mensagem a ser inserida em função do tamanho do arquivo de áudio. O objetivo é introduzir dados de forma quase transparente, de tal maneira que a detecção por terceiros seja pouco provável. O método empregado foi concebido tanto para a ocultação da mensagem em um arquivo de som, como também para garantir a recuperação praticamente inalterável dos dados. O áudio é decomposto em doze níveis mediante a escolha de uma *wavelet*-mãe, os dados são codificados e ocultados nos diferentes níveis segundo o critério do usuário. Para um melhor espalhamento dos dados em cada nível são utilizadas senhas alfanuméricas de tamanho proporcional à quantidade de caracteres ingressados em cada um dos níveis ou sub-blocos. Além dos níveis elegidos, outros parâmetros se fazem presentes para a inserção da mensagem tais como: coeficientes da *wavelet* e posição decimal dos coeficientes, os quais formarão o grupo das chaves-estego, que posteriormente será empregada na recuperação da mensagem. A implementação computacional foi realizada no Matlab<sup>®</sup>. Simulações com arquivos de áudio de diferentes tamanhos foram realizadas, inserindo-se mensagens que variam no número de caracteres, obtendo-se resultados da modificação percentual do som expressos em tabelas. Mudanças que se apresentam em arquivos de áudio após a inserção dos dados, podem ser medidas mediante algum sistema ou algoritmo que detecte a variação do som. Também pode ser usado, não como um decisor, mas simplesmente como referência, o ouvido, devido à subjetividade que apresenta o Sistema Auditivo Humano. Baseadas no esquema da esteganografia, aplicações comerciais foram desenvolvidas para a proteção e segurança da mídia digital, para garantir a autenticidade e arquivos, assim como a proteção e direitos autorais em arquivos digitais. (436 palavras).

Abstract of Dissertation presented to UFPE as a partial fulfillment of the requirements for the degree of Master in Electrical Engineering.

**A steganographic system implementation for text inserting in audio files.**

**Jinnett Pamela Carrión Casiera**

March/2009

Advisors: Dr. Hélio Magalhães de Oliveira, Dr. Ricardo Menezes Capello de Souza

Area of Concentration: Communications / Digital Signal Processing.

Keywords: Information hiding, steganography, data, audio signals, wavelet.

Number of Pages: 152

The art and science of communicating in a way that hides the existence of a plaintext is known as steganography, which has the aim of sending a trade secret in a non-suspicious manner. A brief overview on the steganography history leads automatically to examine its steps forward, from the earliest and naïve schemes to modern digital applications. As technology progresses, new models of steganography have been proposed that exploits the features and weakness of particular digital formats. Standard techniques for data hiding are presented, besides the wavelet-based approach proposed in this thesis. This novel two-step steganography approach combines plaintext encryption by a standard cryptosystem followed by the embedding of the encrypted data in an audio file. The study is focused on inserting short texts into wav files– the data input is performed in the wavelet transform components of the audio, by means of a technique that replaces the most significant decimal positions of the wavelet coefficients, constraining the text length according to the audio file extent. The goal is to perform an almost transparent data inserting in such a way that the detecting by potential eavesdroppers is very unlikely. This low-throughput stego-method was conceived not only to hide a message in an audio file, but also to guarantee an unchanged data retrieval. The audio signal is decomposed in twelve levels after a mother-wavelet choice; data are encoded and embedded at different decomposing levels according to the user choice. In order to guarantee a better data scattering in each level, alphanumeric passwords of length proportional to the number of inserted characters in each sub-block are used. Besides the selected levels, further parameters are required to embed the text, including: the wavelet coefficients, the chosen decimal positions, which comprise the stego-key that will be used in the recovering of the hidden text. This novel stego-tool was fully implemented using Matlab™. Computer simulations with several audio files with different lengths were performed, by inserting texts varying the number of characters, thereby obtaining the percent change rate of the sound file. Changes in audio files due to the text embedding can be assessed by some dedicated system or algorithm that is able to distinguish minor sound alterations. The human hearing can also be used not exactly as a decision-making, but merely as a reference, due to the high-subjectivity of the human auditory system. Many commercial steganography-based schemes have been developed to offer protection and security for digital multimedia, so as to testify the authenticity of files, or to protect copyrighted digital files. (417 words).