INSTITUTO MILITAR DE ENGENHARIA

CAP ANGELO MARCIO CARDOSO RIBEIRO BORZINO

UM ESTUDO SOBRE A CRIPTOANÁLISE DE SINAIS DE VOZ CIFRADOS NO DOMÍNIO DA FREQÜÊNCIA

Dissertação de Mestrado apresentada ao Curso de Mestrado em Engenharia Elétrica do Instituto Militar de Engenharia, como requisito parcial para obtenção do título de Mestre em Ciências em Engenharia Elétrica.

Orientador: Prof. José Antonio Apolinário Jr., D. Sc.
Co-orientador: Dirceu Gonzaga da Silva, M.C.

Rio de Janeiro
2007

INSTITUTO MILITAR DE ENGENHARIA

CAP ANGELO MARCIO CARDOSO RIBEIRO BORZINO

UM ESTUDO SOBRE A CRIPTOANÁLISE DE SINAIS DE VOZ CIFRADOS NO DOMÍNIO DA FREQÜÊNCIA

Dissertação de Mestrado apresentada ao Curso de Mestrado em Engenharia Elétrica do Instituto Militar de Engenharia, como requisito parcial para obtenção do título de Mestre em Ciências em Engenharia Elétrica.

Orientador: Prof. José Antonio Apolinário Jr., D.Sc.

Co-orientador: Dirceu Gonzaga da Silva, M.C.

Aprovada em 02 de fevereiro de 2007 pela seguinte Banca Examinadora:

Prof. José Antonio Apolinário Jr., D.Sc. do IME - Presidente

Dirceu Gonzaga da Silva, M.C. do IME

Prof. José Antônio Moreira Xexéo, D.Sc. do IME

Prof. Ernesto Leite Pinto, D.C. do IME

Prof. Antonio Carlos Gay Thomé, Ph.D. da UFRJ

Rio de Janeiro
2007

AGRADECIMENTOS

Primeiramente, a Deus, por me dar forças e confiança para enfrentar todas as dificuldades da vida.

Ao Instituto Militar de Engenharia, por me acolher e possibilitar a realização do curso de Mestrado.

À Seção de Engenharia Elétrica do IME, por prover os recursos necessários à pesquisa e ao desenvolvimento desta dissertação.

Ao Cel Apolinário, pelos ensinamentos que eu obtive, por me orientar mostrando grande conhecimento nos assuntos discutidos, por me auxiliar em todas as etapas desta pesquisa, pela confiança a mim depositada e por me estimular a participar de simpósios e outros eventos.

Ao Maj Dirceu, por transmitir seus conhecimentos na área de voz, por fornecer todo o material necessário, pela paciência e pelas idéias apresentadas, contribuindo para o enriquecimento do trabalho.

Ao Cel Miscow, por participar desta pesquisa com a elaboração de teste subjetivo de criptofonia e pelas sugestões e conselhos dados.

À minha esposa, pela paciência e pelo apoio dado em casa para eu conseguir terminar este trabalho. Sem esse apoio, seria difícil concluí-lo. Sou grato também por se preocupar quando você percebia que eu ficava muito tempo "grudado" no computador.

À minha filha, pela compreensão das horas que tive de passar trabalhando. Sempre que eu me sentia cansado, ficava feliz em pensar que podia descansar passando algum tempo com você.

Ao meu filho, por também compreender o tempo que tive de ficar "afastado" e por mostrar admiração pelo meu trabalho, sendo mais uma pessoa a me estimular a

continuar as pesquisas até o fim.

À minha mãe, pelo amor, pelos ensinamentos e por me fazer perceber que o estudo é importante para o sucesso na vida profissional. À minha irmã, também pelo amor e pelo carinho que tem por mim. Ao meu pai (em memória), por possibilitar que eu desse os primeiros passos na vida para me tornar feliz com a profissão escolhida.

E não poderia deixar de agradecer ao meu amigo Mário (em memória) que, a despeito do aumento da concorrência, me induziu a prestar concurso para o IME junto com ele. Posso então dizer que a minha graduação e esta dissertação tiveram sua contribuição. Obrigado pela oportunidade.

Enfim, a todos que contribuíram de forma direta ou indireta para a conclusão deste trabalho.

RESUMO

Esta dissertação apresenta uma contribuição à criptoanálise de sinais de voz cifrados no domínio da freqüência. Uma introdução geral sobre criptofonia é dada de forma que detalhes mais específicos relativos aos misturadores implementados usando DFT e banco de filtro do tipo DFT uniforme são providos. São feitas comparações entre eles a fim de verificar as vantagens e desvantagens de cada um.

O objetivo da criptoanálise é tornar inteligível uma informação cifrada, sem o prévio conhecimento da chave (permutação, neste caso) usada no processo de embaralhamento. A técnica utilizada neste trabalho foi a busca em um *codebook* formado pela quantização de vetores que representam a potência espectral de quadros extraídos de sinais contendo todos os fonemas da Língua Portuguesa. Propostas de melhoria dessa técnica são apresentadas e resultados mostram um aumento na inteligibilidade dos sinais criptoanalisados.

É ainda proposta uma medida de desempenho objetiva com a finalidade de determinar a inteligibilidade de um sinal que teve suas sub-bandas de freqüência permutadas; essa nova medida mostrou significativa correlação com a avaliação subjetiva.

Por fim, foi realizada uma análise de desempenho para mostrar que os efeitos deletérios de um canal HF degradam mais o sinal criptoanalisado que a presença de ruído branco aditivo.

ABSTRACT

This dissertation presents a contribution to the cryptanalysis of speech signals ciphered in the frequency domain. A brief overview on criptophony is presented and more specific details concerning those scramblers implemented using DFT and uniform DFT filter banks are provided. Comparisons between them are carried out to evaluate their advantages and disadvantages.

The goal of cryptanalysis is making a ciphered information intelligible without the previous knowledge of the key (permutation in our case) used in the scrambling process. The technique used in this work is based on the search over a codebook formed from the quantization of vectors representing the spectral power of frames obtained from signals containing all phonemes of the Portuguese Language. Improvements of this technique are proposed and the results show an increase in the intelligibility of the cryptanalysed signals.

It is also proposed an objective performance measure aiming to assess the intelligibility of an speech signal having their sub-bands permuted; this novel measure showed a significant correlation with subjective evaluation.

At last, a performance analysis was carried out to show that the deleterious effects of an HF channel degrade more the cryptanalised signal than the presence of additive white noise.