INSTITUTO MILITAR DE ENGENHARIA

1º TEN GLEYSON AZEVEDO DA SILVA

CONTRIBUIÇÃO À CRIPTOANÁLISE DE SINAIS DE VOZ CIFRADOS NO DOMÍNIO DO TEMPO

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: José Antonio Apolinário Jr., D.Sc.
Co-orientador: Prof. Luíz Pereira Calôba, D. Ing.

Rio de Janeiro
2006

INSTITUTO MILITAR DE ENGENHARIA

1º TEN GLEYSON AZEVEDO DA SILVA

CONTRIBUIÇÃO À CRIPTOANÁLISE DE SINAIS DE VOZ CIFRADOS NO DOMÍNIO DO TEMPO

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: José Antonio Apolinário Jr., D.Sc.

Co-orientador: Prof. Luíz Pereira Calôba, D. Ing.

Aprovada em 06 de Fevereiro de 2006 pela seguinte Banca Examinadora:

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

Prof. Luíz Pereira Calôba, D. Ing. da COPPE/UFRJ

Prof. Marcílio Castro de Matos, D. C. do IME

Prof. Rex Nazaré Alves, D. Sc. do IME

Prof. Sergio Lima Netto, Ph. D. da COPPE/UFRJ

Rio de Janeiro
2006

Ao Criador,
ao meu filho, Lucas Gabriel,
aos meus pais,
à minha amada.

AGRADECIMENTOS

Ao Instituto Militar de Engenharia, por mais uma vez me acolher e permitir a realização deste curso de Mestrado.

Ao Centro de Pesquisa em Segurança das Comunicações (CEPESC), por suportar e contribuir significativamente para que esse projeto fosse levado a cabo.

Ao professor José Antonio Apolinário Jr, pela orientação, apoio, confiança e por me ensinar a gostar da pesquisa e do trabalho acadêmico. Como conseqüência de sua orientação, o IME produziu mais um mestre oriundo da latitude zero.

Ao professor Luís Pereira Calôba, pela orientação e desprendimento com que se dedicou à co-orientação dessa dissertação. Suas sugestões, observações e confiança foram uma dose extra de motivação para a conclusão desse trabalho.

Ao Major Dirceu Gonzaga da Silva, *"amigo mais chegado que um irmão"* (Pv. 18:24), pelo seu desprendimento e amizade ímpar. A sua colaboração com idéias, sugestões e, principalmente, com o seu próprio tempo, nunca será esquecida.

Ao professor Juraci Ferreira Galdino, pelas análises, críticas e sugestões. Certamente o bom humor e o "sangue nordestino" facilitaram demais o estreitamento desses laços de amizade.

Aos meus amigos do mestrado, por terem sido companheiros nos melhores e piores momentos desse curso. Em particular, ao amigo Arthur (Larusso), por me ensinar que uma grande amizade se constrói mais baseada em caráter do que em tempo de convivência.

Aos meus pais, pois sem eles nada disso, nem minha própria existência seria possível. A cada dia, tomo mais conhecimento do quanto sou importante para eles e é maravilhoso trilhar a estrada dessa descoberta.

Ao meu filho, Lucas Gabriel, por representar o meu maior motivo em prosseguir. As horas que seu pai gastou longe de você, definitivamente, não foram em vão.

Este não poderia faltar: *usg aks u kzu vvj gnt osg.*

Por fim, mas em primeiro lugar, ao meu Senhor, Jesus Cristo, por me possibilitar viver a cada dia conhecendo minhas limitações e contemplando a Sua grandeza, representada pelo sacrifício de si mesmo em prol de todos.

"...porque sem mim, nada podeis fazer."
(palavras de JESUS CRISTO em João 15:5)

"Talvez não tenhamos conseguido fazer o melhor, mas lutamos para que o melhor fosse feito... Não somos quem deveríamos ser; não somos quem iremos ser; mas, graças a Deus, não somos o que éramos!"

MARTIN LUTHER KING

RESUMO

Essa dissertação representa uma contribuição aos métodos existentes de criptoanálise de sinais de voz cifrados no domínio do tempo. A técnica escolhida para estudo foi a *Permutação de Segmentos Temporais*, também conhecida pela sigla em inglês TSP (*Time Segment Permutation*), cujo processo de cifragem consiste no embaralhamento de blocos de N segmentos temporais em uma abordagem de "salto por janela".

Como o objetivo da criptoanálise é tornar inteligível uma informação cifrada sem ter o prévio conhecimento da chave (permutação, neste caso) usada no embaralhamento, a motivação da pesquisa desenvolvida neste trabalho foi apresentar um procedimento, de aplicação prática, que oferecesse melhor desempenho do que os métodos existentes.

Para atingir o propósito desejado, uma investigação das seguintes características, utilizadas com sucesso em várias aplicações, foi realizada à luz da criptoanálise temporal: os coeficientes *cepstrum*, as *freqüências do espectro de linha* (*Line Spectral Frequencies* - LSF) e uma conjugação entre os coeficientes *cepstrum* obtidos através dos coeficientes preditores (LPCC) e os coeficientes *cepstrum* obtidos pela DFT (*Discrete Fourier Transform*) (LFCC). Outrossim, foram empregadas com o mesmo escopo a quantização vetorial (QV), a combinação de classificadores e um estudo preliminar de criptoanálise temporal através de redes neurais.

Visando verificar objetivamente o desempenho de cada característica e ferramenta, foi proposta uma taxa de acerto com base na continuidade temporal do sinal decifrado; essa medida objetiva tem mostrado significativa correlação com a avaliação subjetiva.

A aplicação prática de um método de criptoanálise depende da compensação de distorções introduzidas no sinal cifrado no percurso entre o transmissor e a aquisição do sinal pelo criptanalista. Apesar da relevância do efeitos introduzidos por essas distorções, a pesquisa divulgada nessa área faz pouca ou nenhuma menção de como compensá-la. Destarte, foram estudadas duas técnicas de estimação cega de canal: uma baseada na identificação dos zeros do canal e a outra na *subtração da média cepstral* (*Cepstrum Mean Subtraction* - CMS). Por fim, foi observado, através de simulações, que o método proposto aqui é robusto ao ruído aditivo.

ABSTRACT

This dissertation represents a contribution to the existing methods of cryptanalysis of time domain ciphered speech signal. The technique chosen for this investigation is known by its acronym TSP (Time Segment Permutation) which ciphering process consists of scrambling blocks of N time segments in a *"hopping window"* approach.

Since the objective of a cryptanalysis is to make a ciphered information understandable without the prior knowledge of the key (permutation in this case) used in the scrambling procedure, the motivation of the research developed in this work is the presentation of a procedure, of practical application, that could offer a better performance when compared to existing methods. The resorting of the permuted segments in each block is carried out by means of an exhaustive search which choice takes into account the permutation with the minimal spectrum distance between borders of adjacent segments.

In order to accomplish the desired goal, an investigation on the following features, successfully used in a number of applications, applied to the problem of time scrambling cryptanalysis was carried out: cepstrum, Line Spectral Frequencies (LSF), and a concatenation of cepstral coefficients obtained through linear prediction coefficients (LPCC) and the cepstral coefficients obtained from the Discrete Foutier Transform (DFT)(LFCC). Besides these features, vector quantization and the combination of classifiers were also addressed. Besides these features, were also addressed in the same way the vector quantization, the combination of classifiers and a preliminary study of cryptanalysis by neural network.

Aiming to objectively assessing the performance of each feature and tool, a new performance rate was proposed, based on the temporal continuity of the cryptanalyzed signal; this new objective measure has shown a significant correlation with subjective evaluation. In light if this measure, the feature presenting the best results was a combination of the cepstrum with pitch information. Moreover, from the simulations, it was observed that the use of vector quantization as well as the combination of different classifiers has shown prospective results.

The practical application of a cryptanalysis method depends on the compensation of distortions introduced in the ciphered signal during the path from the transmitter to the signal acquisition by the cryptanalyst. Although being this distortion quite significant, little or nothing has been published concerning the possible compensation. Therefore, two blind channel estimation techniques were studied in an attempt to apply them to the problem of scrambled speech cryptanalysis: the first one is based on the identification of channel zeros and the second one based on the so-called CMS (Cepstrum Mean Subtraction). It was also observed, through computer simulations, that the methods proposed here are robust to additive noise.