CRIPTOANÁLISE DE SINAIS DE VOZ CIFRADOS POR PERMUTAÇÃO DE SEGMENTOS TEMPORAIS BASEADA EM DISTÂNCIAS ESPECTRAIS

José Antonio Apolinário Junior
CIGE - Divisão de Engenharia - C.P. 020191 CEP 70.001 Brasília/DF

Henrique Sarmento Malvar
UnB - Departamento de Engenharia Elétrica - C.P. 04591 CEP 70.919 Brasília/DF

Sumário - **Este trabalho apresenta um esquema de criptoanálise de um dos métodos de criptofonia: a permutação de segmentos temporais. Este esquema é baseado no levantamento das características do espectro do sinal nas extremidades dos segmentos e na comparação das características do final de um segmento com as do início de um possível segmento adjacente por meio de medidas de distância espectral. É feita um breve introdução aos métodos de criptofonia e às medidas de distância espectral. É apresentado o algoritmo de criptoanálise e o bom desempenho do mesmo é mostrado por meio de medidas objetivas dos resultados obtidos em simulações feitas.**

1. Introdução

A CRIPTOANÁLISE é o ramo da criptologia que tenta extrair a informação existente numa mensagem cifrada sem conhecer-se a chave. Quando a mensagem em claro for um sinal de voz, o processo de cifrar esta mensagem (transformá-la num criptograma) é conhecido como criptofonia. A criptoanálise possui aplicações restritas a uns poucos aficcionados e, principalmente, a órgãos e agências governamentais que tratam esta disciplina de maneira sigilosa.

A criptofonia utilizando a permutação de segmentos temporais, conhecida também pela sigla em inglês TSP ("Time Segment Permutation"), é uma técnica tradicional usada em "scramblers" (misturadores de voz) que, embora sozinha ofereça um grau relativamente pequeno de privacidade, não apresenta uma criptoanálise conhecida ou pelo menos amplamente divulgada.

O presente trabalho tem por objetivo apresentar uma proposta de criptoanálise de sinais de voz cifrados por permutação, bloco a bloco, de segmentos temporais de tamanho fixo ("TSP jumping window"). Trata-se de uma contribuição inicial para um possível sistema automático de criptoanálise de um sinal de voz que passou por um "scrambler".

A idéia básica é a escolha da permutação que apresenta a menor soma das distâncias espectrais das bordas de segmentos adjacentes. Bons resultados são obtidos com simulações do esquema proposto.

Serão mencionados na Seção 2 os diversos métodos de criptofonia, dentre os quais destaca-se aquele de interesse para este artigo. A seguir, encontra-se na Seção 3 um breve resumo das medidas de distância espectral que foram efetivamente usadas. A Seção 4, algoritmo de criptoanálise, apresenta o esquema proposto que consiste de uma preparação do sinal, da reordenação dos segmentos e de uma melhoria após a reordenação. A Seção 5 mostra alguns resultados obtidos em simulações bem como uma sucinta análise dos mesmos. Finalmente, a Seção 6 formaliza algumas conclusões.

2. Permutação de Segmentos Temporais

Apresentamos, inicialmente, uma classificação dos sistemas de criptofonia segundo o método utilizado [Cabral Jr., 1987]:

CSI (Criptofonia por Segmentos de Informação):
- no domínio da freqüência (CSI-F): divide o espectro em faixas e embaralha-as;
- no domínio do tempo (CSI-T): permutação de segmentos temporais;
- bidimensionais (CSI-FT): cifra tanto na freqüência quanto no tempo;

CBB (Criptofonia Bit a Bit): cifra os bits de um sinal digitalizado;

CCI (Criptofonia de Características Informativas): extrai parâmetros do sinal para cifrá-los.

A primeira classe (CSI) é, pois, composta dos "SCRAMBLERS". Os equipamentos das classes seguintes (CBB e CCI) são conhecidos como "COMSEC", apresentam um maior grau de segurança e um preço mais elevado.

A técnica de interesse para este trabalho, permutação de segmentos temporais de tamanhos fixos e "jumping window" é um exemplo de CSI-T que inclue diferentes variantes tais como a de segmentos de tamanhos variáveis e aquela que usa um bloco com um número fixo de segmentos e a saída por sorteio: o próximo elemento de entrada ocupa o local do segmento sorteado para transmissão e novo sorteio ocorre; a cada sorteio, um teste é feito para evitar que um segmento não fique no bloco por um tempo superior ao correspondente a dois tamanhos de bloco ("sliding window").

Observamos na Figura 1 os conceitos de bloco e segmentos. Os segmentos foram permutados dentro de um bloco; para que isto possa ser realizado, é necessário que todos os segmentos deste bloco sejam armazenados numa memória antes de serem transmitidos numa ordem diferente da original. Isto implica num retardo total de comunicação igual a duas vezes o tamanho do bloco (transmissão e recepção). Este retardo é uma das limitações do processo, bem como o número de segmentos em cada bloco: um

número grande de segmentos diminuiria a inteligibilidade residual e aumentaria a resistência à criptoanálise, mas ao mesmo tempo causaria expansão de banda, necessidade de um sincronismo mais preciso e um efeito mais acentuado de superposição de segmentos (a ser comentada na seção 4) quando o sinal passa por um canal. Uma combinação de 8 segmentos num bloco de tamanho igual a 256 ms parece ser bem razoável para aplicações práticas e tais valores foram implementados nas simulações efetuadas.

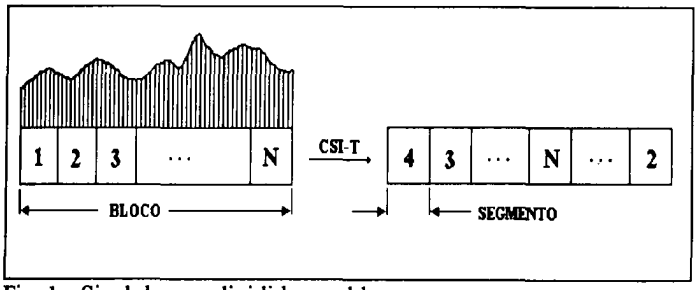


Fig. 1 - Sinal de voz dividido em blocos e segmentos.

Num sistema deste tipo, sabemos que o número máximo de permutações de N elementos é N!. Entretanto, devido à alta inteligibilidade de um sinal de voz permutado de maneira mais "simples", somente um número K << N! pode ser considerado efetivo. A estimação deste número efetivo de chaves K é difícil de definir ou avaliar pois o conceito de inteligibilidade é bastante subjetivo [Jayant, 1987]. Pode-se afirmar [Cabral Jr., 1987] que para um sistema CSI-T usando um bloco com 8 segmentos, temos que das 8! = 40320 maneiras de se permutar os segmentos, somente cerca de 3000 são efetivas.

O sincronismo é um outro problema merecedor da atenção daqueles que trabalham com criptofonia ou com sua criptoanálise. Ele pode ser inicial (todas as informações necessárias são enviadas numa salva no início da transmissão), contínuo (as informações são enviadas continuamente através de uma portadora piloto que ocupa uma pequena faixa da banda de áudio) ou intercalado (a transmissão do sinal de voz é periodicamente interrompida, total ou parcialmente e por uma pequena fração de segundo, para a transmissão de bits de sincronismo).

Fazendo-se um levantamento dos equipamentos de criptofonia produzidos pelas grandes empresas mundiais [Jane's Military Communications, 1991-92], observou-se que: 32,5% dos sistemas de criptofonia produzidos são CSI (a grande maioria bidimensionais e alguns com diferentes variantes), 37,6% CCB, 22,1% CCI e 7,8% não foram especificados ou não se encaixam exatamente na divisão apresentada. Estes valores mostram que, apesar do crescimento dos sistemas digitais, os "scramblers" ocupam, ainda, uma posição muito importante no mercado internacional.

3. Medidas de Distância Espectral

Uma medida de distância espectral é a visualização através de um número não negativo do quanto o espectro de um sinal está próximo ou não do espectro de um outro sinal. Desde quando a predição linear tornou-se amplamente difundida como modelo para a produção de voz, o estabelecimento de uma medida de distância espectral baseada em dois conjuntos de coeficientes LPC ("linear prediction coefficients") passou a merecer uma grande atenção por parte dos pesquisadores. Neste trabalho, é de interesse considerar-se a distância entre os espectros do final e do início de dois segmentos de sinal de voz para verificar-se o quanto os mesmos se assemelham.

Dada a necessidade de levantar-se os coeficientes LPC numa análise a curto tempo para que seja possível comparar os espectros em dois instantes de tempo (antes e após a transição dos segmentos), optou-se, então, pela utilização de uma estrutura reticulada ("lattice") que, além de oferecer a possibilidade de obtenção dos coeficientes de modo adaptativo (amostra a amostra), apresenta encadeamento de seções idênticas, coeficientes com magnitude menor que 1, teste de estabilidade por inspeção e obtenção dos coeficientes direto das amostras de voz sem um cálculo intermediário da função de autocorrelação [Cowan e Grant, 1985]. Os coeficientes da estrutura reticulada, usualmente chamados coeficientes de reflexão $\{\mathbf{k}_i\}$, independem da ordem **p** do filtro e podem ser transformados em coeficientes $\{\mathbf{a}_i\}$ (LPC) ou $\{\mathbf{c}_i\}$ (cepstrais) [Markel e Gray, 1976].

O algoritmo utilizado para a estimação dos coeficientes de reflexão neste trabalho foi uma versão normalizada do RLSL ("Recursive Least-Squares Lattice") conhecida como SQNLSL ("Square-Root-Normalized Least-Square Lattice"). Este algoritmo apresenta uma diminuição da complexidade das recursões e uma melhoria nas propriedades numéricas das variáveis [Cowan e Grant, 1985].

Encontra-se na literatura [Itakura, 1975, Gray e Markel, 1976, Tribolet, Rabiner e Sondhi, 1979, Gray, Buzo, Gray e Matsuyama, 1980, De Souza e Thomsom, 1982 e Brown e Rabiner, 1982] várias medidas de distância espectral. Todas elas são amplamente usadas em processamento de voz e particularmente em criptofonia [Sridharan, Dawson e Goldburg, 1991] para medir objetivamente inteligibilidade residual e qualidade de voz recuperada. Serão usadas neste trabalho as distâncias Euclideana, de Itakura e cepstral.

A distância Euclideana será calculada a partir dos vetores **d** e **e** que contém os coeficientes de reflexão estimados nos dois instantes de interesse (à direita ou no final de um segmento e à esquerda ou no início de um outro)[1]. A distância Euclideana simples (não ponderada) é dada pelo produto interno do vetor diferença **(d-e)** por ele mesmo. Brown e Rabiner [1982] sugerem a inclusão da informação de energia do sinal na medida de distância espectral. Esta informação (adotado aqui o módulo do logaritmo da razão de variâncias) será ***adicionada*** à distância não ponderada através de uma constante de escalonamento (α). A distância Euclideana usada neste trabalho é, pois, dada por:

$$\mathbf{de(D,E)} = \sqrt{(\mathbf{d}-\mathbf{e})^t.(\mathbf{d}-\mathbf{e})} + \alpha.\left|\log\frac{\mathbf{R(D)}}{\mathbf{R(E)}}\right| \qquad (1)$$

[1] Os coeficientes da extremidade direita de um segmento foram calculados rodando-se um filtro SQNLSL no sentido direto das amostras do segmento e os da extremidade esquerda rodando-se o mesmo filtro no sentido inverso.

onde: R(D) é a variância do sinal no instante D e R(E) é a variância em E.

A medida de distância espectral desenvolvida por Itakura [Itakura,1975] e conhecida como razão de verossimilhança logarítmica ("log likelihood ratio") tem, provavelmente, sido a mais popular medida de distância baseada nos coeficientes LPC. Uma variante desta distância de Itakura foi usada neste trabalho [Apolinário Jr., 1993] e é dada por:

$$di(D,E) = \frac{1}{2}\log\left[\frac{Res(X_D,K_E)}{Res(X_D,K_D)}\cdot\frac{Res(X_E,K_D)}{Res(X_E,K_E)}\right] + \alpha\left|\log\frac{R(D)}{R(E)}\right| \quad (2)$$

onde $Res(X_I,K_J)$ é o resíduo obtido quando rodamos uma estrutura reticulada nas amostras X_I usando os K's constantes e estimados a partir das amostras X_J.

A constante α, tanto para a distância Euclideana quanto para a de Itakura, deverá ser ajustada para obter-se o melhor resultado para cada sinal. O valor $\alpha = 2$ é, em geral, um bom início para constatar-se de imediato uma melhoria de desempenho em relação ao caso $\alpha = 0$, que corresponde ao uso só dos coeficientes LPC.

Usando os coeficientes cepstrais, é definida uma distância (cepstral) que está associada a uma média quadrática das diferenças de dois espectros em magnitude logarítmicos [Markel e Gray, 1976] e é dada por:

$$dc(D,E) = \left[c_D(0) - c_E(0)\right]^2 + 2.\sum_{i=1}^{p}\left[c_D(i) - c_E(i)\right]^2 \quad (3)$$

onde os c's são os coeficientes cepstrais em D e E, e p é a ordem do modelo. Observa-se que em (3) já encontra-se embutida a informação de energia (c's índice zero).

4.Algoritmo de Criptoanálise

O esquema de criptoanálise proposto nesta seção é aplicável num sinal de voz que foi cifrado pela permutação de N segmentos temporais de mesmo tamanho dentro de blocos transmitidos sequencialmente. Será assumido neste trabalho que N = 8. Esta informação não é facilmente obtida diretamente do sinal. Na prática, existe ainda a incerteza sobre o método utilizado: "JUMPING WINDOW" ou "SLIDING WINDOW". Contudo, observa-se que nos manuais de vários equipamentos ("SCRAMBLERS") de grandes fabricantes constam o método, o tamanho do segmentos em milisegundos e o número N de segmentos por bloco.

Deseja-se, incialmente,obter um arquivo contendo o sinal de voz criptofonado onde sabe-se que seu início coincide com o início de um segmento e conhece-se exatamente o número de amostras de cada segmento. Para isto são estimados os coeficientes LPC (k's e variância) amostra a amostra, via SQNLSL, do arquivo original e do arquivo invertido no tempo. Isto feito, é calculado e gravado num outro arquivo (sinal.dst) as distâncias entre as amostras adjacentes conforme a Figura 2. Estas distâncias são obtidas da seguinte maneira: com os coeficientes estimados do arquivo original, obtém-se a distância entre os coeficientes na amostra atual e os coeficientes estimados na amostra anterior ($\mathbf{d}_d$); no caso dos coeficientes estimados a partir do arquivo invertido no tempo, reinverte-se os mesmos inicialmente e obtém-se uma nova distância ($\mathbf{d}_i$). Será considerada como distância (variação do especto do sinal no instante daquela amostra em relação ao instante da amostra anterior) o maior valor entre $\mathbf{d}_d$ e $\mathbf{d}_i$. A idéia é a obtenção de picos de distância que possam indicar variações abruptas no espectro do sinal (prováveis transições de segmentos).

De posse do arquivo do sinal original e deste arquivo contendo as possíveis transições, consegue-se visualizar os segmentos e obter-se o tamanho dos mesmos. Um exemplo de um sinal CSI-T e suas correspondentes distâncias espectrais amostra a amostra são mostrados na Figura 3.

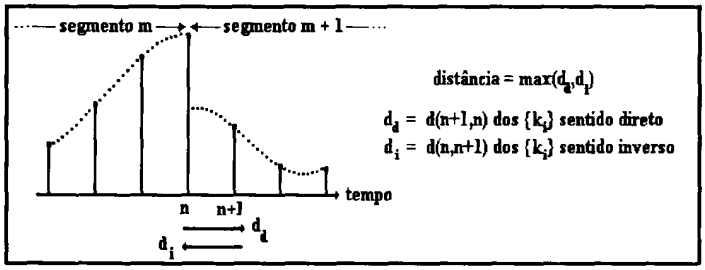


Figura 2 - Obtendo as transições de segmentos.

Observa-se na Figura 3 que, se fosse estabelecido um certo limiar para decidir sobre a existência ou não de uma transição de segmentos, haveria um considerável número de erros ao longo do sinal. Estes erros são conhecidos classicamente como de dois tipos: existia uma transição que não foi detectada ("miss") e não existia uma transição que foi detectada ("false alarm"). Entretanto, como sabemos que todos segmentos possuem o mesmo tamanho, podemos fazer a correlação do sinal school.dst com um trem de impulsos periódicos. À medida que o trem de impulsos "desliza" haverá um certo momento onde a correlação será máxima, ou seja, os impulsos estarão em cima das transições dos segmentos. Fazendo-se um período variável, dentre limites estabelecidos por uma inspeção visual, e escolhendo-se aquele que corresponde à maior correlação, pode-se ter uma boa estimativa do tamanho do segmento, bem como do número de amostras entre o início do arquivo e o início do primeiro segmento. Entretanto, não é conhecido o início de um bloco. Esta informação, embora fundamental, não chega a ser uma preocupação, pois podemos executar a reordenação dos segmentos supondo que o um bloco inicia-se no primeiro segmento obtido, depois no segundo e assim por diante até o oitavo. Desta forma, um dos resultados será o melhor e corresponderá a uma suposição correta do início do bloco. O único inconveniente é efetuar a criptoanálise para oito arquivos sem saber qual deles está preparado adequadamente. Mas, o tempo de processamento é pequeno para o caso de oito segmentos e, portanto, este inconveniente não justifica uma análise do sincronismo do sinal cifrado para descobrir-se o primeiro segmento a priori.

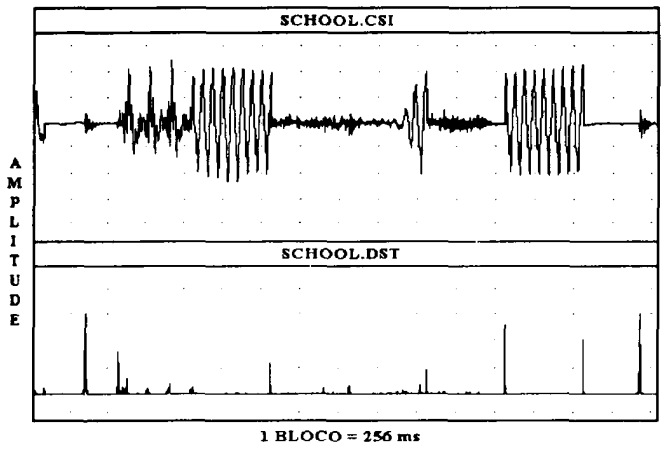


Figura 3 - Sinal de voz criptofonado CSI-T e suas distâncias espectrais.

O algoritmo apresentado na Figura 4 mostra como será processada a reordenação dos segmentos. Para cada bloco (8 segmentos) lido são estimados os coeficientes $\{k_i\}$ à direita e à esquerda de cada segmento. Para os coeficientes à esquerda, roda-se um filtro SQNLSL do final para o início do segmento. Os coeficientes à direita são obtidos com o mesmo filtro rodando do início para o final do segmento. Os coeficientes estimados são armazenados e as distâncias do final para o início de dois segmentos são calculadas e armazenadas numa matriz contendo todas as distâncias possíveis entre os segmentos do bloco.

```
/* ALGORITMO CSITOVOZ (CRIPTOANÁLISE DE CSI-T) */
INÍCIO CSITOVOZ (ENTRA:SINAL.CSI, SAI:SINAL.VOZ)
  "DECLARAÇÃO DE ARQUIVOS E VARIÁVEIS";
  "ABERTURA DE ARQUIVOS";
  "LEITURA E ESCRITA DE CABEÇALHOS";
  "INICIALIZAÇÃO DE VARIÁVEIS";
  ENQUANTO NÃO (FIM DE ARQUIVO)
    "LER UM BLOCO DO ARQUIVO DE ENTRADA";
    PARA SEG DE I ATÉ NR_SEGS PASSO I
      "CALCULAR Kd (COEFICIENTES À DIREITA DO
       SEGMENTO )";
      "CALCULAR Ke (COEFICIENTES À ESQUERDA DO
       SEGMENTO)";
    FIM-PARA;
    "CALCULAR AS DISTÂNCIAS d[i][j] (DIR SEG i PARA ESQ
                                          SEG j)";
    "ACHAR A PERMUTAÇÃO DE MENOR DISTÂNCIA (USANDO
     A FUNÇÃO VISIT ( ) ";
    "GUARDAR OS COEFICIENTES DO FINAL DO BLOCO";
    "REORDENAR OS SEGMENTOS E ESCREVER NO ARQUIVO
     DE SAÍDA";
  FIM-ENQUANTO;
  "FECHAR ARQUIVOS";
FIM {CSITOVOZ}.
```

Figura 4 - Algoritmo de criptoanálise (BLOCO com NR_SEGS = 8 segmentos).

A seguir, são testadas as 8! (40320) permutações possíveis (busca exaustiva) entre segmentos do mesmo bloco. É usado para isto a função recursiva visit( ) sugerida por Sedgewick [Sedgewick, 1946]. Para cada permutação, acha-se uma distância total que corresponde a soma das distâncias das transições de segmentos desta permutação. Dentre as 8! permutações, é escolhida aquela que apresenta a menor distância total. A permutação escolhida é guardada num vetor que será a ***chave*** para a reordenação dos segmentos. Uma vez efetuada a reordenação, é escrito o bloco no arquivo de saída e o processamento continua com a leitura do próximo bloco.

Em casos reais, quando o sinal criptofonado passa por um canal, ocorre uma superposição de segmentos, ou seja, o final de um segmento avança, por efeito do canal, para o início do segmento seguinte. O resultado é o aparecimento de um ruído indesejável que degrada a inteligibilidade do sinal quando recuperado. Para minimizar este efeito, são normalmente zeradas algumas amostras do final de cada segmento (cerca de 1 a 2 ms) antes da transmissão [manuais dos equipamentos Cryptophon 1100 da Brown, Boveri & Company, Ltd. e TST 7595 da Tele Security Timmann]. Apesar disto, ainda notamos esta superposição de segmentos. Este efeito é percebido diretamente na forma de onda como alguns picos nas transições dos segmentos ou ouvindo o sinal ("zumbido" de fundo). Para melhorar o resultado pode-se, então, diminuir a amplitude das primeiras amostras de cada segmento. Isto irá permitir uma melhoria na qualidade do sinal criptoanalisado pois, como foi observado em experimentações, o "zumbido" causado pelos possíveis vales que ocorrem quando o sinal tem amplitude alta prejudica menos a inteligibilidade do que o "zumbido" causado pelos picos de superposição.

5. Resultados Experimentais

Os resultados são apresentados por meio de medidas objetivas de desempenho do quanto o sinal criptoanalisado aproxima-se do sinal original, apesar de poder-se conjecturar que o objetivo da criptoanálise é a obtenção do conteúdo da mensagem e não a recuperação perfeita do sinal de voz que foi cifrado. Neste particular, embora não tenham sido feitas medidas subjetivas de uma maneira formal, todos os sinais criptoanalisados ficaram ***inteligíveis*** para as pessoas consultadas.

Os sinais de voz usados nos testes passaram por um simulador de CSI-T "jumping window" onde o sinal de entrada é dividido em blocos de 8 segmentos de 256 amostras e os segmentos são "embaralhados" por meio de uma permutação uniforme [Apolinário Jr., 1993]. Foram utilizados os seguintes arquivos de voz :

- SCHOOL.VOZ: voz masculina, idioma inglês, gravada em fita K-7;
- SINTO.VOZ : voz feminina, idioma português e gravada de um aparelho de televisão;
- TELEF2.VOZ : voz masculina, idioma português e proveniente de um canal telefônico;
- VEGA2.VOZ : voz feminina, idioma inglês e gravada em fita K-7. Apresenta uma certa constância na constância na sua intensidade (amplitude quase constante).

Observamos, a seguir, a Tabela 1 que apresenta uma medida de distorção espectral relativa (foi chamada de distorção para não confundir com as medidas de distância espectral usadas na criptoanálise e corresponde à distância Euclideana

não ponderada dos coeficientes $\{a_i\}$ estimados segmento a segmento dos sinais original e criptoanalisado em relação ao original) para os sinais cifrados verso cada medidas de distância.

	SCHOOL	SINTO	TELEF2	VEGA2
EUCLIDEANA	29,4 %	36,2 %	29,1 %	7,2 %
DE ITAKURA	33,8 %	32,5 %	26,1 %	18,6 %
CEPSTRAL	23,3 %	24,0 %	21,3 %	5,3 %

Tabela 1 - Distorção espectral relativa (um valor para cada distância espectral usada).

Uma outra medida objetiva de desempenho, a ***taxa de acertos*** (número de segmentos recolocados em seus locais de maneira acertada pelo número total de segmentos do sinal), é mostrada na Tabela 2.

	SCHOOL	SINTO	TELEF2	VEGA2
EUCLIDEANA	70,3 %	51,0 %	52,5 %	89,7 %
DE ITAKURA	61,7 %	58,3 %	51,2 %	66,2 %
CEPSTRAL	72,7 %	65,6 %	63,1 %	91,2 %

Tabela 2 - Taxa de acertos (# segmentos certos / # total de segmentos).

6. Conclusão

Dos resultados obtidos na Seção 5, concluimos que o método é eficaz na sua tarefa de obter inteligibilidade de um sinal cifrado. Verifica-se, também, que a medida espectral que apresentou a melhor performance foi a cepstral. Por outro lado, a distância de Itakura, embora seja tradicionalmente considerada uma boa medida de distância espectral, não é muito adequada ao esquema proposto uma vez que a simples distância Euclideana mostrou-se melhor na maioria dos testes.

Os resultados apresentados neste artigo dizem respeito a passagem do sinal cifrado por um canal ideal. No caso do sinal passar por um canal que apresente uma distorção de fase acentuada, como é o caso de um canal telefônico típico, torna-se necessário fazer-se uma equalização do canal para podermos obter resultados próximos dos aqui mostrados [Apolinário Jr., 1993].

Finalmente, resta mencionar que a grande maioria dos "scramblers" atuais cifram o sinal de voz em mais de uma dimensão (CSI-FT), sendo a permutação temporal somente parte do processo. Nestes casos a criptoanálise torna-se mais complexa e esta tarefa seria uma extensão natural deste trabalho.

Referências

Apolinário Jr., José Antonio., Criptoanálise de Sinais de Voz Cifrados por Permutação de Segmentos Temporais, Dissertação de Mestrado, UnB, Brasília, Junho de 1993.

Brown, M. K. **e Rabiner**, L. R., On the Use of Energy in LPC-Based Recognition of Isolated Words, in "The Bell System Technical Journal", vol. 61, n°. 10, dezembro 1982, pp 2971-2987.

Brown, Bovery & Company, Ltda., Manual do Cryptophon 1100, Suiça.

Cabral Jr., Euvaldo F., Uma Incursão pelos Domínios da Criptofonia, in "Revista Militar de Ciência e Tecnologia", vol IV, n°. 2, abril/junho 1987, pp 26-52.

Cowan, C.F.N. **e Grant**, P.M., Adaptive Filters, Englewood Cliffs, Prentice-Hall, 1985.

De Souza, Peter **e Thomson**, Peter J., LPC Distance Measures and Statistical Tests with Particular Reference to the Likelihood Ratio, in "IEEE Transactions on Acoustic, Speech, and Signal Processing", vol. ASSP-30, n°. 2, abril 1982, pp 304-315.

Gray Jr., Augustine H. **e Markel**, John D., Distance Measures for Speech Processing, in "IEEE Transactions on Acoustic, Speech, and Signal Processing", vol. ASSP-24, n°. 5, outubro 1976, pp 380-391.

Gray, Robert M., **Buzo**, Andrés, **Gray** Jr., Augustine H. **e Matsuyama**, Yasuo, Distortion Measures for Speech Processing, in "IEEE Transactions on Acoustic, Speech, and Signal Processing", vol. ASSP-28, n°. 4, agosto 1980, pp 367-376.

Itakura, Fumitada, Minimum Prediction Residual Principle Applied to Speech Recognition, in "IEEE Transactions on Acoustic, Speech, and Signal Processing", vol. ASSP-23, n°. 1, fevereiro 1975, pp 67-72.

Jane's Military Communications, 1991-92.

Jayant, N.S., Effective Number of Keys in a Voice Privacy System Based on Permutation Scrambling, in "AT&T Techical Journal", vol. 66, n°.1, janeiro/fevereiro 1987, pp 132-136.

Markel, J.D. **e Gray** Jr., A.H., Linear Prediction of Speech, Berlin, Springer-Verlag, 1976.

Sedgewick, Robert, Algorithms, USA, Addison-Wesley Publishing Company, 1946 (2a. edição em 1988).

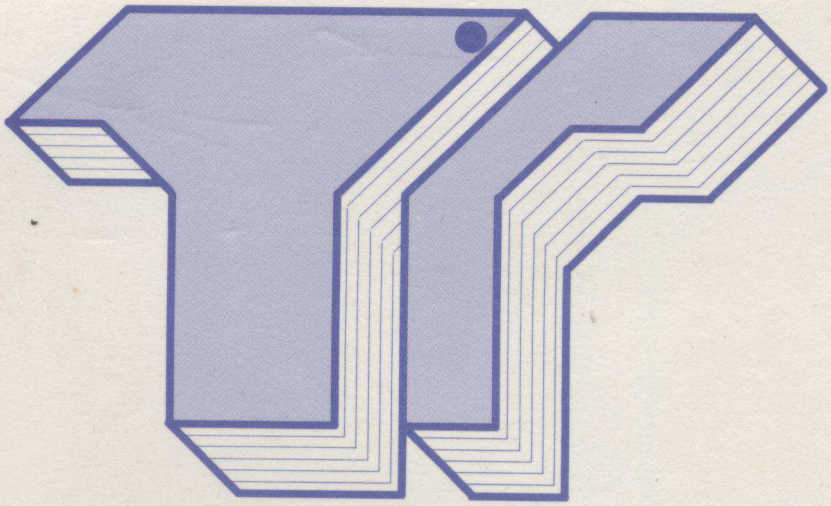
Sridharan, S., **Dawson**, E. e **Goldburg**, B., Fast Fourier Transform Based Speech Encryption System, in "IEE Proceedings-I", vol. 138, n°. 3, junho 1991, pp 215-223.

Tele Security Timmann, Manual do TST 7595, Alemanha.

Tribolet, José M., **Rabiner**, Lawrence R. e **Sondhi**, Man Mohan, Statistical Properties of an LPC Distance Measure, in "IEEE Transactions on Acoustic, Speech, and Signal Processing, vol. ASSP-27, n°. 5, outubro 1979, pp 550-558.

11º SIMPÓSIO BRASILEIRO DE TELECOMUNICAÇÕES
06 A 10 DE SETEMBRO DE 1993
NATAL - RN

11º SBT



NATAL - RN

VOLUME I

PROMOÇÃO:

SOCIEDADE BRASILEIRA DE TELECOMUNICAÇÕES
UNIVERSIDADE FEDERAL DO RIO GRANDE DO NORTE