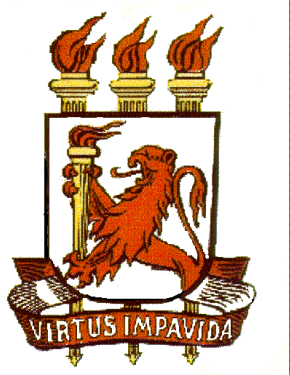


Baixa taxa de dados em áudio baseada em Esteganografia

Universidade Federal de Pernambuco

Programa de Pós-graduação em Engenharia Elétrica



Pamela Carrión*
Hélio Magalhães de Oliveira
Ricardo Campello de Souza

PPGEE

PROGRAMA DE PÓS-GRADUAÇÃO
EM ENGENHARIA ELÉTRICA

UFPE

SBSeg - Gramado
Setembro 2008

Esteganografia

Arte e a ciência da comunicação em segredo.

Objetivo Geral

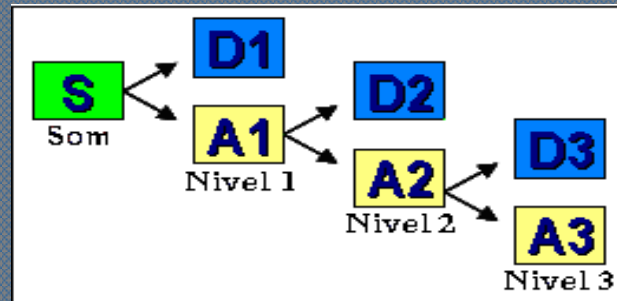
Ocultar uma mensagem de texto em um arquivo de áudio com formato .wav mediante transformadas wavelet, de maneira que o som não sofra modificações detectáveis.

Esteganografia vem do grego *steganos* (escondido) e *gráphos* (escrita), i.e. a escrita oculta.

Enquanto a Criptografia encarrega-se em tornar uma mensagem não compreensível, a Esteganografia a torna despercebida. Combinando o potencial das duas logra-se consolidar um sistema eficiente.

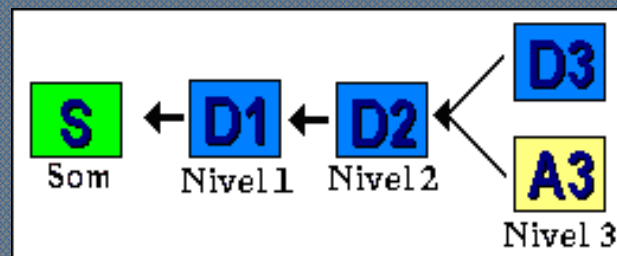
A Transformada de Wavelet como ferramenta para inserção de dados

Mediante a decomposição do sinal via wavelets, geram-se *aproximações* e *detalhes*; o processo é repetitivo, e as aproximações são subdivididas para cada nível.

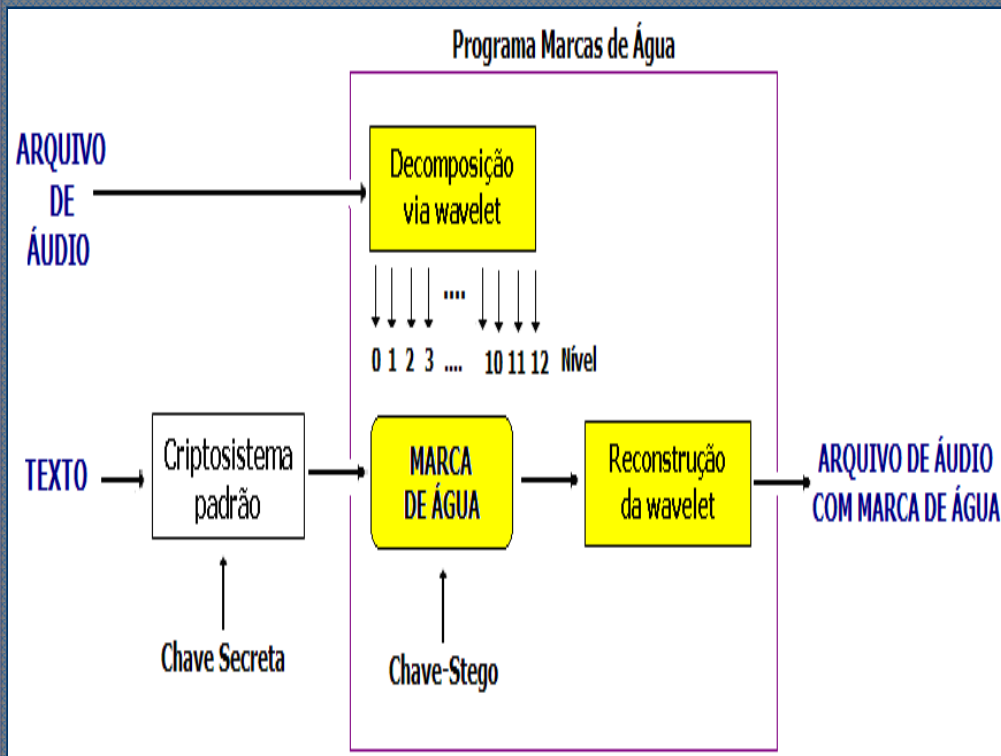


Devido a esta característica é possível implementar a inserção dos dados em diferentes níveis.

A partir de suas componentes, pôde-se recompor o sinal original: este processo é chamado de Wavelet Discreta Inversa.



Idéias sobre a Implementação



Baseia-se na transformação do sinal hóspede mediante uma wavelet-mãe escolhida pelo usuário.

O texto previamente cifrado por um criptosistema conhecido será inserido no sinal cobertor.

O sinal de áudio é decomposto em 12 níveis, e a inserção dos dados é realizada nos níveis escolhidos empregando a *chave-stego* a qual é também requerida para a decifragem.

Finalmente, o sinal é reconstruído usando-se a assinatura.

Implementação

Inserção de dados:



Som sem dados

Mensagem

Mensagem em código
Ascii

77 101 110 115 97 88 97

Wavelet Nível

Níveis, Senha(s), Lugar de inserção

Nível 1

Nível 2 [77 101 110]

Nível 3

Nível 4 [115 97]

Nível 5

Nível 6 [88]

Nível 7

Nível 8

Nível 9 [97]

Nível 10

Nível 11

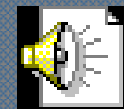
Nível 12

Lugar de inserção: 1

Matriz gerada da decomposição do som via wavelet

| | | |
|----|-------------------|---|
| 1 | -0.07873535156250 | 0 |
| 2 | -0.06811523437500 | 0 |
| 3 | -0.07755078125000 | 1 |
| 4 | 0.01135253906250 | 0 |
| 5 | -0.00878906250000 | 0 |
| 6 | 0,10167120960430 | 1 |
| 7 | -0.02969296053811 | 0 |
| 8 | 0.00535163823652 | 0 |
| 9 | 0.02261498738658 | 0 |
| 10 | 0.11049484203253 | 1 |

Senha



Som com dados

Implementação

Recuperação dos dados:



Som com dados

SENHAS-STEGO

- Tipo de Wavelet.
- Tamanho da mensagem.
- Número de níveis.
- Nível(s) onde o texto foi ingressado.
- Tamanho dos sub-blocos de texto.
- Senha(s).
- Lugar de inserção do texto.

Matriz gerada da decomposição do som via wavelet

| | |
|----|-------------------|
| 1 | -0.07873535156250 |
| 2 | -0.06811523437500 |
| 3 | -0.07755078125000 |
| 4 | 0.01135253906250 |
| 5 | -0.00878906250000 |
| 6 | 0,10167120960430 |
| 7 | -0.02969296053811 |
| 8 | 0.00535163823652 |
| 9 | 0.02261498738658 |
| 10 | 0.11049484203253 |

Mensagem em código
Ascii

77 101 110 115 97 88 97

Aquí hay un
mensaje escondido
que sólo la persona
indicada lo podrá
descifrar

Mensagem

Conclusões

- Ocultação de dados em áudio mediante as transformadas wavelets, e o principal objetivo é que o áudio passe despercebido ante a percepção humana.
- Baseado na Esteganografia foram desenvolvidas aplicações envolvendo marcas de água para proteção de direitos autorais, assinaturas digitais, e autenticação de arquivos.
- A combinação da Esteganografia com Criptografia reforça a segurança, evitando que intrusos tenham conhecimento da informação oculta.

Referências

- 1]** J.C. Judge, "Steganography: Past, Present, Future," Lawrence Livermore National Laboratory, U.S. Department of Energy UCRL-ID-151879 University of California, 2001.
- 2]** N.F. Johnson, S. Jajodia, "Exploring steganography: Seeing the unseen," *IEEE Computer* 31 (2), pp.26–34, 1998.
- 3]** M.A.T. Alsalami, M.M. Al-Akaidi, "Digital Audio Watermarking: Survey," *17th European Simulation Multiconferece, ESM*, 2003.
- 4]** USA Today, San Francisco, Reuters "Researchers: No secret Bin Laden messages on sites" URL: www.usatoday.com/life/cyber/tech/2001/10/17/bin-laden-site
- 5]** J. Dittmann, C. Kraetzer, ECRYPT-European Network of Excellence in Cryptology, "Audio Benchmarking Tools and Steganalysis," Jan., 2006.
- 6]** M.K. Johnson, S. Lyu, H. Farid, "Steganalysis of Recorded Speech", *Proc. SPIE*, 5681, pp. 664-672, 2005.
- 7]** W. Bender, D. Gruhl, N. Morimoto, A. Lu, "Techniques for data hiding." *IBM Systems Journal*, 35 (3&4), 1996, pp.313-336.
- 8]** R. Chandramouli, N. Memon, "Analysis of LSB image steganography techniques," *Proc. ICIP* 3, pp. 1019–1022, 2001.