PROTÓTIPO DE SOFTWARE PARA OCULTAR TEXTOS COMPACTADOS EM ARQUIVOS DE ÁUDIO UTILIZANDO ESTEGANOGRAFIA

Acadêmico: André Kobuszewski
Orientador: Prof. Francisco Adell Péricas

ROTEIRO

- Introdução
- Fundamentação teórica
- Requisitos
- Especificação
- Implementação
- Resultados e discussão
- Conclusão
- Extensões

INTRODUÇÃO

- Os computadores vêm assumindo uma crescente importância como meios de armazenamento, processamento e troca de informação entre várias instituições da nossa sociedade

- A segurança está relacionada à necessidade de proteção contra o acesso ou manipulação de informações confidenciais por elementos não autorizados

OBJETIVOS DO TRABALHO

- Desenvolver um protótipo de software que utiliza técnicas de esteganografia em conjunto com a compressão de Huffman, para ocultar textos em arquivos de áudio

FUNDAMENTAÇÃO TEÓRICA

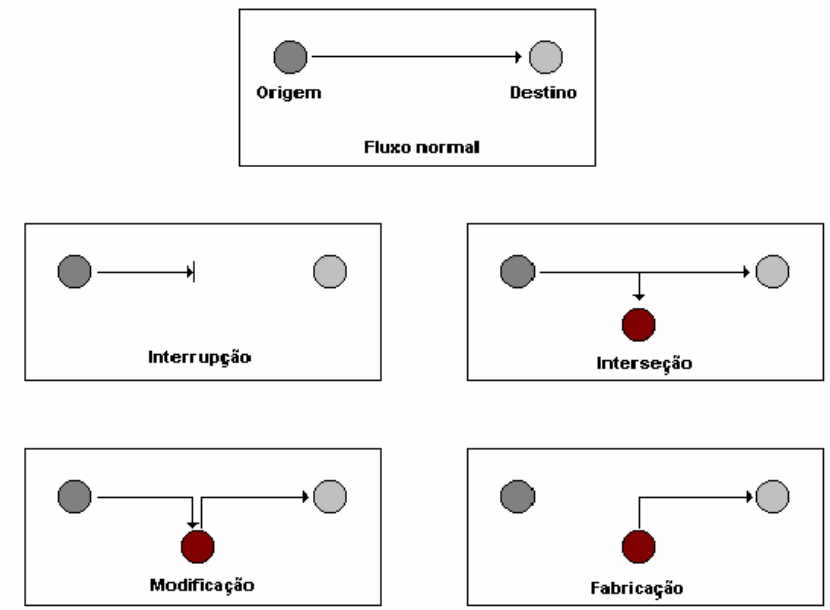
SEGURANÇA DAS INFORMAÇÕES

- Comunicação segura:
  - sigilo
  - integridade
  - autenticação

AMEAÇAS E ATAQUES

- Principais objetivos de ameaças:
  - interrupção
  - interseção
  - modificação
  - fabricação

- Tipo de ameaças
  - passivas
  - ativas



MECANISMOS DE PROTEÇÃO

- Técnicas de proteção de dados:
  - criptografia: escrita em códigos
    - chave simétrica: mesma chave (DES)
    - chave assimétrica: duas chaves (RSA)
  - esteganografia: comunicação secreta
    - sons, imagens, textos, sinais etc.
  - assinatura digital: autenticidade de documentos

ESTEGANOGRAFIA

- ***estegano*** = esconder, mascarar, e ***grafia*** = escrita
- Histórico
  - "As Histórias", de Heródoto (século V a.C)
  - Segunda Guerra Mundial (século 20)

Exemplo:

Apparently neutral's protest is thoroughly discounted and ignored. Isman hard hit. Blockade issue affects pretext for embargo on by products, ejecting suets and vegetable oils

Pershing sails from NY June 1.

ESTEGANOGRAFIA: MÉTODO LSB

- Distribui a informação utilizando os bits menos significativos do arquivo

Exemplo:

Amostra de um arquivo de som:

```
200       53        2         195       54        69        191       56

11001000  00110101  00000010  11000011  00110110  01000101  10111111  00111000
```

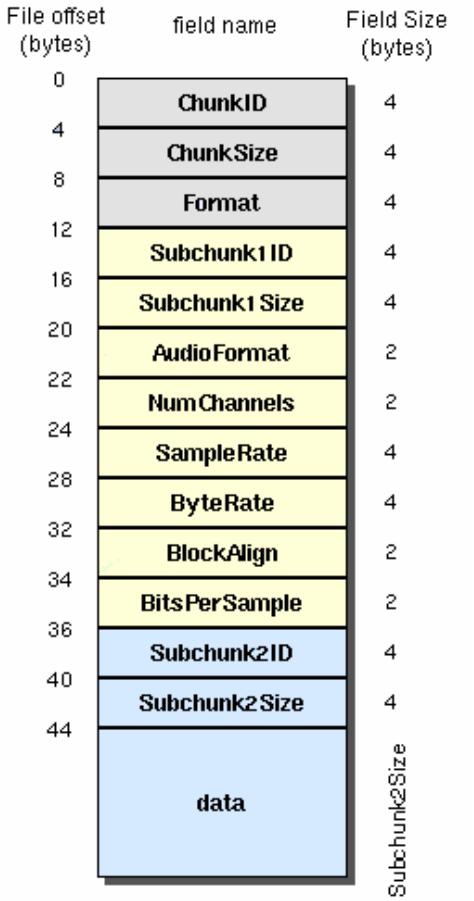
Deseja-se ocultar o byte 109 (01101101):

```
11001000  00110101  00000011  11000010  00110111  01000101  10111110  00111001

200       53        3         194       55        69        190       57
```

ARQUIVOS DE ÁUDIO

- Digitalização do som
- Formatos de arquivo
- Arquivos *wave*
  - cabeçalho
  - área de dados



COMPRESSÃO DE DADOS

- Compressão sem perda: a informação pode ser sempre reconstituída exatamente sem qualquer perda de informação
- Compressão com perda: sacrifica um pouco a integridade da informação em troca de incremento na compressão

COMPRESSÃO DE HUFFMAN

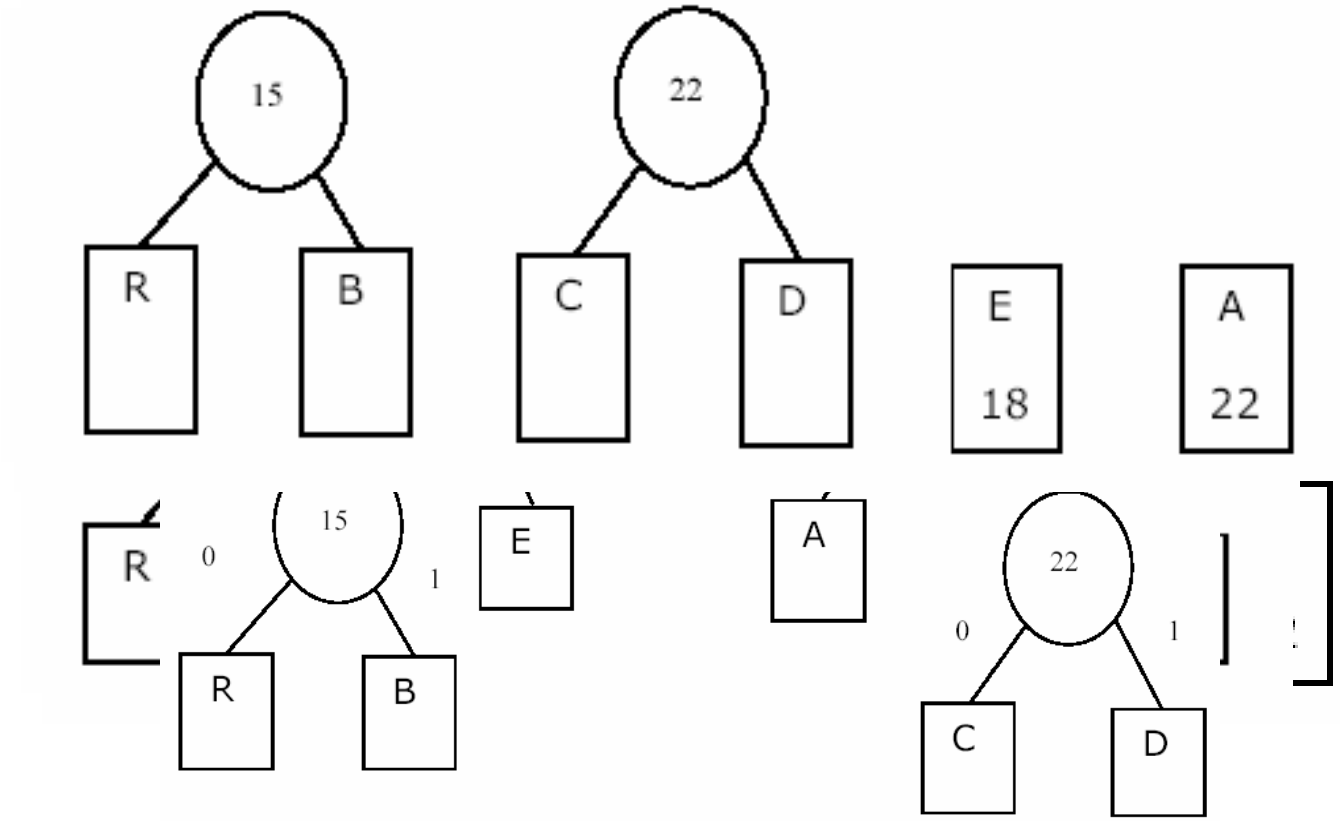
- Método estatístico criado por David Huffman, utilizando estrutura de árvore binária

- Utilização de um código curto para representação de caracteres comuns, e códigos longos para representação de símbolos pouco freqüentes

COMPRESSÃO DE HUFFMAN

Construção da árvore de Huffman:

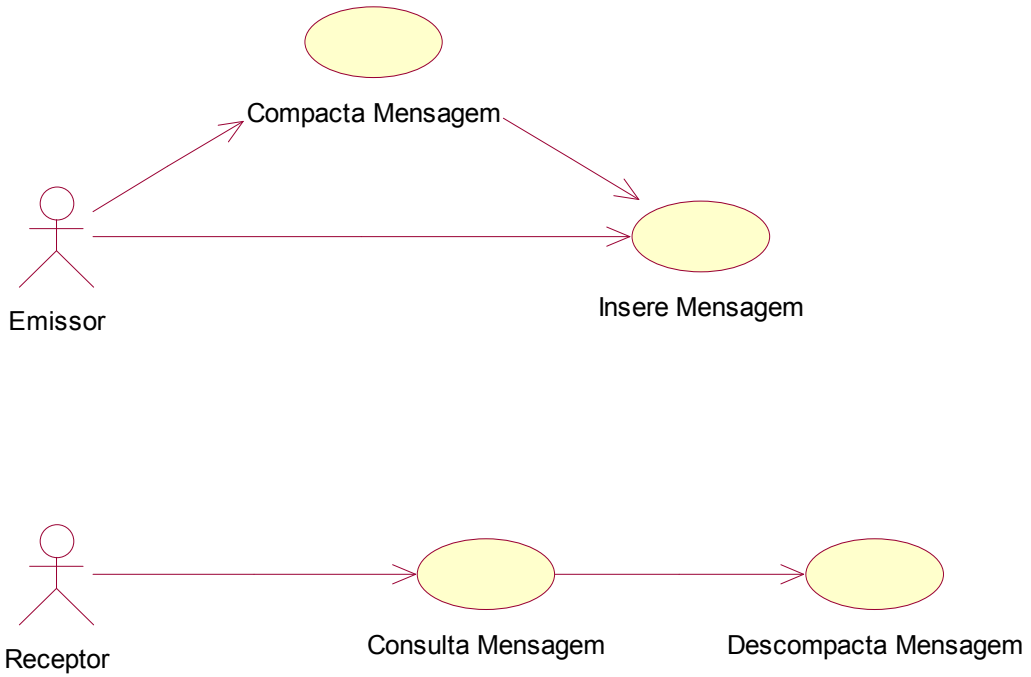
	A	B	C	D	E	R
Freqüência:	22	8	10	12	18	7
Código Binário:	10	001	110	111	01	000



DESENVOLVIMENTO DO PROTÓTIPO: REQUISITOS DO SISTEMA

- Ocultar textos em arquivos de áudio
- Extrair textos esteganografados de arquivos de áudio, descompactando-os quando necessário
- Possibilitar compactação dos textos a serem ocultos

ESPECIFICAÇÃO:
DIAGRAMA DE CASOS DE USO



ESPECIFICAÇÃO:
DIAGRAMA DE CLASSES

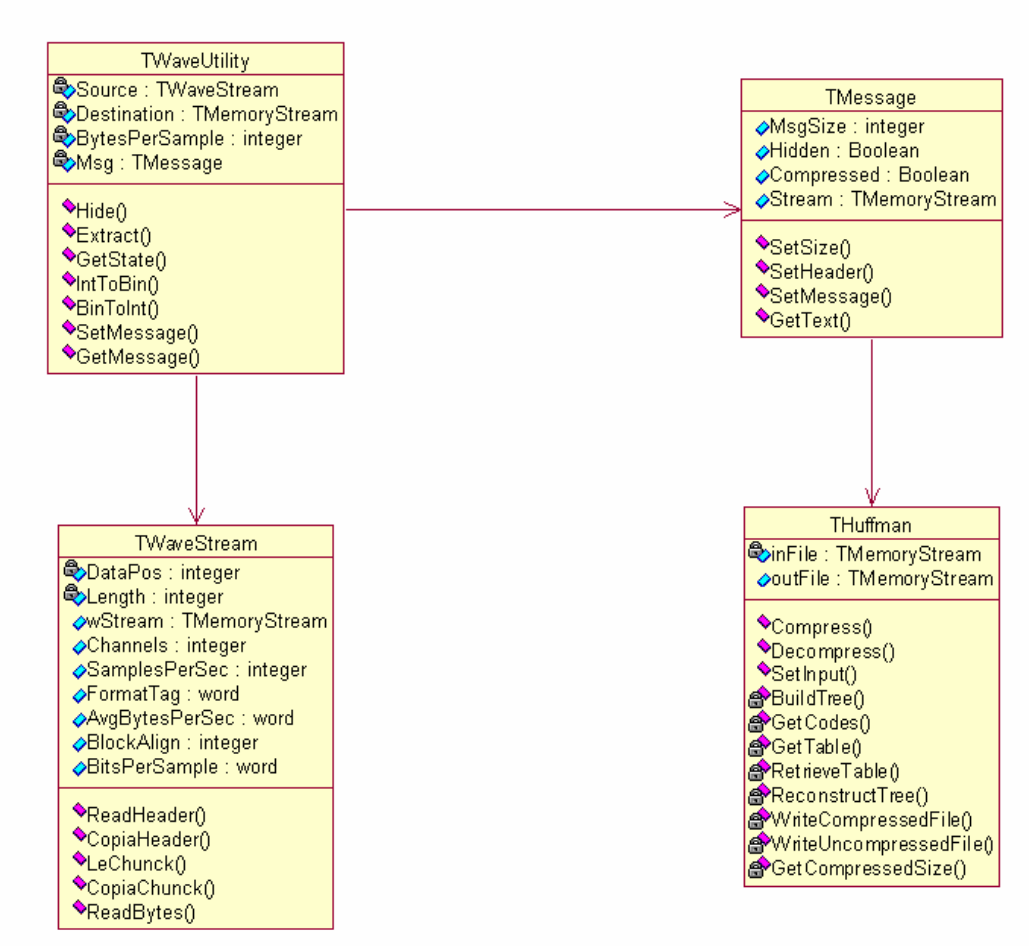
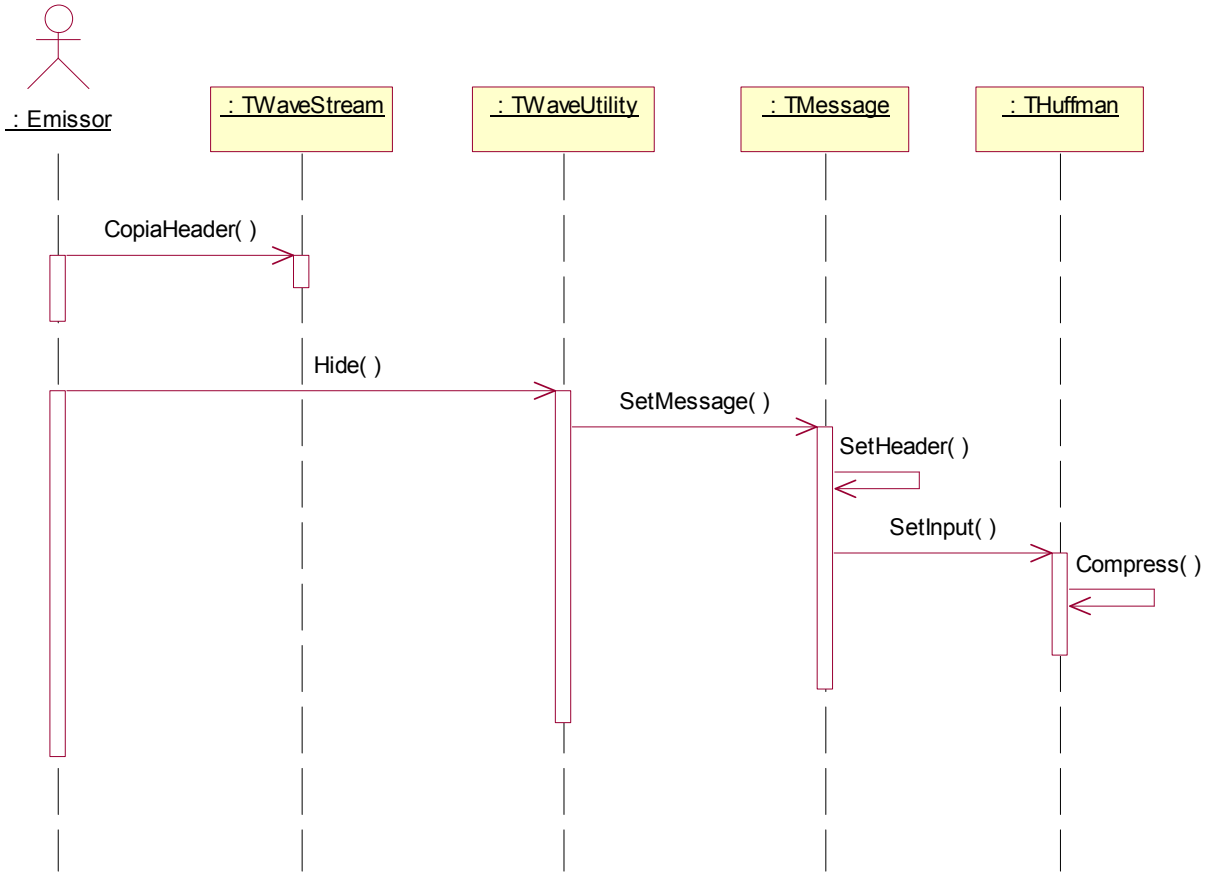


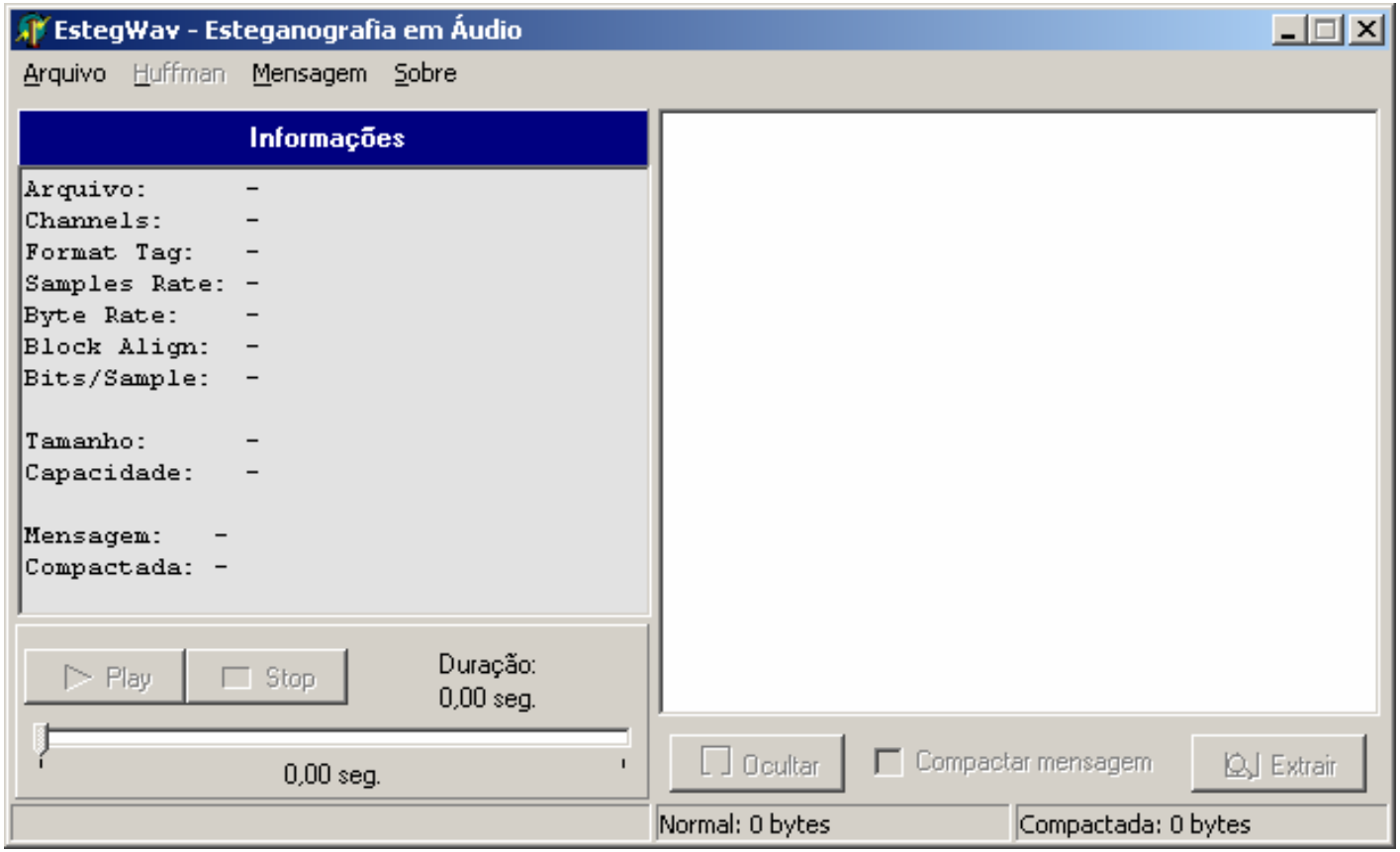
DIAGRAMA DE SEQÜÊNCIA: INSERE MENSAGEM



IMPLEMENTAÇÃO

- Análise do cabeçalho do arquivo *wav*
  - verificação arquivo válido
  - capacidade armazenamento do arquivo
- Inclusão de cabeçalho da mensagem
  - identificador (4 bytes): “@MSG” ou “@CMP”
  - tamanho da mensagem (4 *bytes)*
- Compactação da mensagem

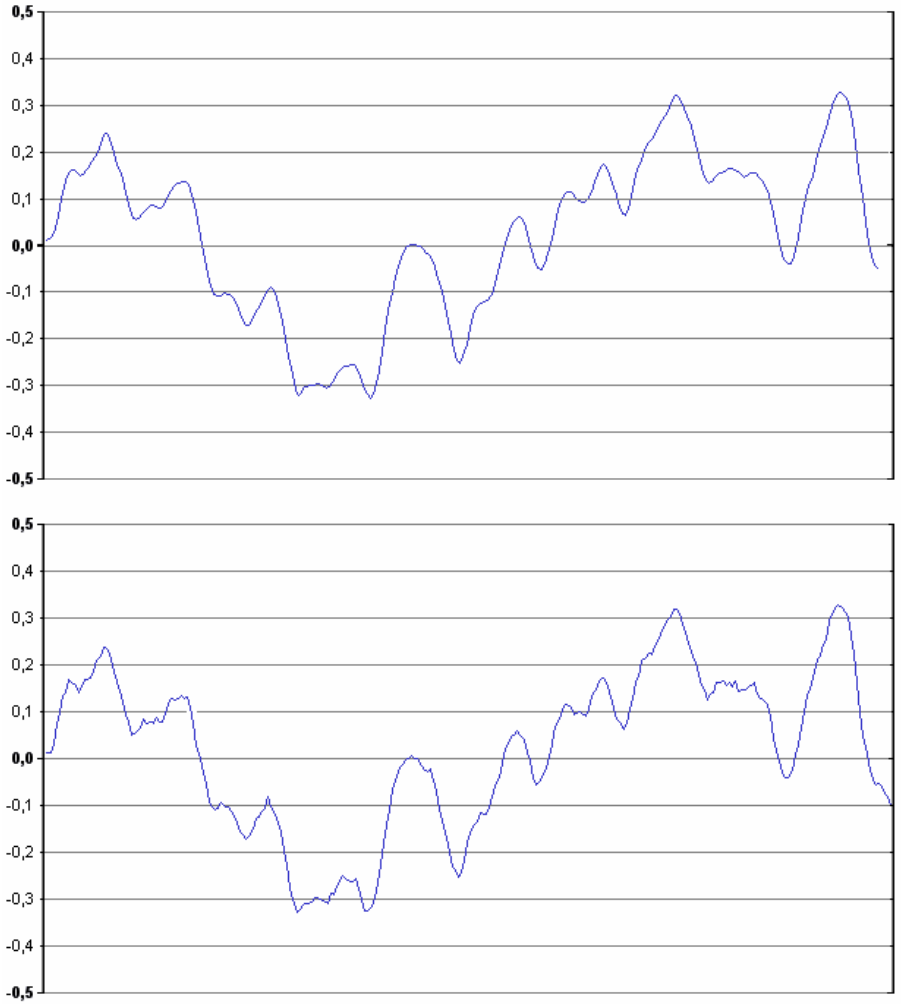
OPERACIONALIDADE DA IMPLEMENTAÇÃO



RESULTADOS E DISCUSSÃO

- Tamanho de amostra
  - 1 byte: 88 bytes
    (11 *bytes* x 8 *bits*)
  - 2 bytes: 176 bytes
    (11 bytes x 8 bits x 2 bytes)

- Pequenas alterações nas ondas do arquivo de áudio, imperceptíveis ao ouvido humano



CONCLUSÕES

- A aplicação da esteganografia mostrou-se bastante eficaz na transmissão de dados de forma segura

- A compressão dos dados permite que sejam utilizados arquivos menores para o armazenamento de informações, e ajuda a tornar sua violação ainda mais difícil

EXTENSÕES

- Aplicação de outras técnicas de esteganografia em arquivos de áudio
- Ocultar outros formatos de arquivos
- Utilização de técnicas de criptografia em conjunto com a esteganografia