****

**Instituto Federal de Educação, Ciência e Tecnologia de Mato Grosso**

Projeto da disciplina de Processamento Digital de Sinais

Matheus Cândido Teixeira e Gustavo Duarte

**Objetivo**

Dado dois áudios, uma mensagem e uma portadora, inserir a mensagem na portadora de tal maneira que o áudio da mensagem não seja detectável pela audição humana somente o áudio da portado será audível, e, dessa forma, criar um sistema de criptografia de áudio. O áudio da mensagem deve ser recuperável a partir do sinal criptografado através de alguma chave .

**Solução**

**Processo de criptografia**

A estratégia para criptografar o áudio pode ser visto na Figura *6*. Cada aspecto do algoritmo esta indicado por indices azuis no fluxograma.

No fluxograma, os índices 1 e 2 são entradas para o algoritmo de criptografia. O primeiro é a mensagem a ser “escondida”, isto é, ser ofuscada do espectro auditivo humano. Com base em diversos trabalhos, a frequência máxima que um ser humano pode ouvir é de 20kHz. Portanto, o áudio a ser escondido deve estar além desta frequência (e mais uma banda de segurança). Já o segundo áudio ofusca o primeiro e, por isso, não precisa ser modificado ou deslocado na frequência. Um exemplo de sinal de mensagem e da portadora pode ser visto na Figura *1*, onde a energia do sinal esta concentrado nas baixas frequências.

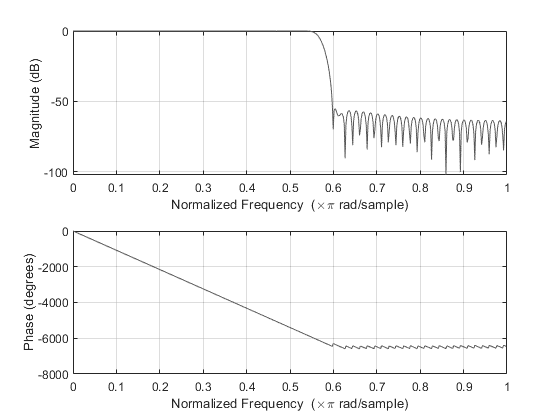
Figura 1: Exemplo do espectro de frequência do sinal de mensagem e do sinal da portadora

|  |  |
| --- | --- |
|  |  |

Fonte: Própria

O terceiro índice, serve para ambos os sinais, uma vez que ambos passam pelo mesmo filtro. O filtro utilizado é um filtro FIR utilizando a janela de Hamming com ordem 120 e *frequência de corte* de rad/s, onde , é a frequência de amostragem dos sinais de áudio. Geralmente, a frequência de amostragem para arquivos MPEG-1 Audio Layer III (MP3) é de 48kHz, 44,1kHz e 32kHz. A aplicação do filtro nos sinais serve para limitar a banda de frequência de ambos e, através desse processo, garantir que os áudios serão recuperados sem corrupção, distorção ou interferência no processo de descriptografia. A amplitude e fase do filtro construído pode ser visualizado na Figura *2*.

Figura 2: Magnitude e Fase do filtro Passa-Baixas FIR



Fonte: Própria

No quarto índice, ocorre a reamostragem dos sinais de áudio. Como explicado no índice um e três, a frequência de amostragem mínima é de 32kHz e com base nos estudos de Nyquist, essa frequência pode representar sinais de até kHz, isto é, metade da frequência de amostragem e a frequência máxima que o aparelho auditivo humano é capaz de detectar é de 20kHz, ou seja, é necessário uma taxa de amostragem () de 40kHz. Como a banda de frequência do áudio recuperado não é grande o suficiente para acomodar o sinal de áudio que deve ser ofuscado é necessário realizar uma reamostragem do sinal. Após realizar a reamostragem, mais precisamente a sobreamostragem, do sinal por um , onde é um inteiro, a frequência de amostragem será de . E na situação anterior, onde a frequência de amostragem era de 32kHz agora será de () kHz e dessa forma torna-se possível armazenar áudios além dos 20kHz com segurança. O espectro do sinal da Figura *1* após a sobreamostragem pode ser visto na Figura *3*.

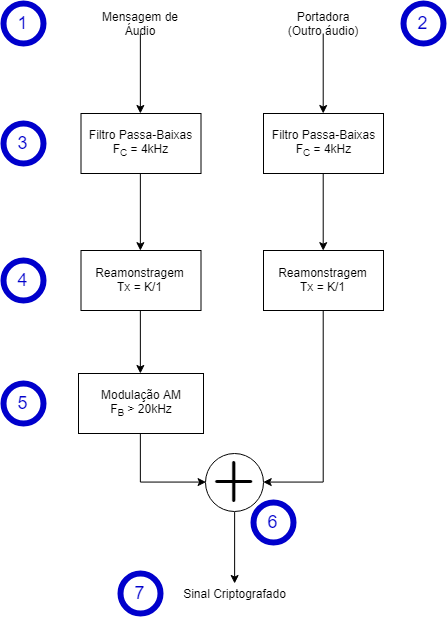
No quinto índice, há uma modulação em amplitude do sinal de mensagem. Isso ocorre apenas deslocar o áudio para a banda desejada. Isso implica em convoluir o sinal por um sinal senoidal no domínio do tempo ou então multiplicá-lo por um pulso no domínio da frequência. Na Figura *4*, é possível ver o sinal sobreamostrado da Figura *3* deslocado na frequência após ser modulado com frequência base de Hz.

No sexto índice, ocorre a soma dos dois áudios. O tamanho dos arquivos não é geralmente do mesmo tamanho, portanto, é necessário expandir o menor vetor até alcançar o tamanho do maior vetor. Isso é feito preenchendo-o com zeros. A consequência desse preenchimento é que, no processo de descriptografia, se o áudio da portadora tiver duração de segundos e o áudio da mensagem tiver segundos e , então os () segundos da mensagem descriptografada não terá som algum.

|  |  |
| --- | --- |
| Figura 3: Sinal de mensagem após a sobreamostragem    Fonte: Própria | Figura 4: Sinal deslocado na frequência    Fonte: Própria |
| Figura 5: Sinal criptografado    Fonte: Própria |  |

Por fim, o sétimo índice é o sinal criptografado. A execução do áudio criptografado será igual ao áudio da portadora, porém o tamanho do arquivo será maior porque embora o áudio da mensagem não seja audível, ainda é necessário armazenar os seus dados. O resultado pode ser visto na Figura *5*, onde a linha vertical indica a frequência máxima na qual o aparelho auditivo humano tem a capacidade de detectar áudio.

Figura 6: Fluxograma do algoritmo de criptografia



Fonte: Própria

**Processo de descriptografia**

O processo de descriptografia se resume em restaurar as modificações realizadas durante a criptografia, porém com algumas simplificações, por exemplo, não é necessário reverter a soma dos sinais como indicado no índice 6 da Figura *6*. Para separar os sinais é realizado uma filtragem do sinal criptografado. O filtro utilizado é um passa-altas com *frequência de corte* de ) rad/s. Após aplicar o filtro apenas a mensagem “escondida” além do 20kHz estará presente no sinal (a portadora foi limitada em banda a 4kHz no processo de criptografia descrito acima, portanto, a filtro passa-altas de 5kHz deve eliminá-la). Isto é realizado nos processos indicados pelos índices 1 e 2 do fluxograma presente na Figura *13*. O sinal de áudio de entrada, o gráfico da amplitude e fase do filtro e o sinal filtrado resultante podem ser vistos nas Figura *7*, Figura *8* e Figura *9*, respectivamente.

Com o sinal isolado, é necessário desfazer os processos de criptografia. No índice 3, é realizado a demodulação do sinal da mensagem. No índice 5 da Figura *6*, a modulação ocorre pela multiplicação de um pulso na frequência desejada já para a demodulação é necessário convoluir por um sinal tal que a convolução desse pelo primeiro sinal que o deslocou seja igual a um pulso, isto é,

Com isso o sinal retornará para a banda original. Porém para achar esse sinal é necessário conhecer o , e, por isso, esse valor pode fazer parte da chave . O áudio demodulado da Figura *9* pode ser visto na Figura *10*.

No processo indicado no quarto índice, ocorre a reamostragem do sinal. Dado um , um inteiro qualquer utilizado no processo de sobreamostragem, ocorre a realização de uma subamostragem do sinal desfazendo a sobreamostragem realizado no processo de criptografia. Com a subamostragem, o sinal também retorna para a frequência de amostragem original. O áudio da Figura *10* subamostrado é mostrado na Figura *11*.

Por fim, no índice 5 do fluxograma o sinal da mensagem é recuperado e é igual ao sinal da mensagem inserido na função de criptografia. O áudio resultante pode ser visto na Figura *12*, note a semelhança da Figura *1* com a Figura *12*.

**Conclusão**

A qualidade do áudio recuperado é semelhante ao áudio da mensagem original. Não há sinais de aliasing e nem um tipo de distorção. O áudio criptografado também não é distinguível audivelmente do áudio da portadora, porém, o arquivo de áudio é consideravelmente maior do que a soma dos áudios da portadora com o áudio da mensagem. Dois parâmetros importantes para recuperar o áudio da mensagem a partir do áudio criptografado é a variável , que é o fator de sobreamostragem para o sinal criptografado, e a frequência da modulação em amplitude (AM), que deve ser superior a 20000 (para não ser audível). Portanto,

Onde

* + é o fator de sobreamostragem
  + É a frequência da portadora para AM
  + é a relação entre as variáveis acima, na qual, pode ser apenas um par ordenado ou a chave para um algoritmo de criptografia de texto mais elaborado.

A implementação dos algoritmos está disponível no link: [Github.com/MatheusCTeixeira](https://github.com/MatheusCTeixeira/PDS/) (Há uma versão para Windows e uma para o Linux)

|  |  |
| --- | --- |
| Figura 7: Sinal Criptografado | Figura 8:Amplitude e Fase do filtro FIR |
| Figura 9:Áudio Filtrado | Figura 10:Áudio Demodulado |
| Figura 11:Áudio Reamostrado | Figura 12:Áudio Recuperado |
|  |  |

Fonte: Própria

Figura 13: Fluxograma do algoritmo de descriptografia



Fonte: Própria