
Universidade Federal de Pernambuco
Departamento de Eletrônica e Sistemas
Matemática Discreta - Exercício Complementar - 2023.1 - I Unidade

Orientações: (i) As questões a seguir devem ser realizadas em grupo: serão definidos trios ou duplas, dependendo do quantitativo de alunos matriculados; (ii) possivelmente, haverá mais de três grupos, de modo que deve haver uma interação entre os grupos 1a, 2a e 3a; 1b, 2b e 3b, e assim por diante. Lendo as questões, ficará mais clara a necessidade dessa interação; (iii) poderá ser utilizada qualquer linguagem de programação para realização das questões; (iv) a data de entrega das questões é o dia 01/08/2023 (uma semana antes do 1º Exercício Escolar); (v) a entrega corresponderá a um relatório em .pdf, contendo as respostas às questões, as imagens e demais dados envolvidos e os códigos elaborados.

1) A esteganografia digital é uma técnica que permite que mensagens (dados digitais) sejam ocultadas em arquivos de imagem e áudio, por exemplo, de modo a serem transmitidas de forma secreta e oportunamente extraídas quando de sua chegada ao destinatário. Uma das técnicas mais conhecidas da esteganografia é a que se baseia na substituição do bit menos significativo (LSB, *least significant bit*) dos pixels de uma imagem por bits que compõem a mensagem que se deseja enviar secretamente. Os itens a seguir orientam para a implementação de mecanismos de inserção e extração de mensagens utilizando a técnica mencionada. Observe as orientações e implemente cada etapa utilizando uma linguagem de programação à sua escolha. **Um grupo de alunos ficará responsável por implementar a fase de inserção da mensagem e outro grupo ficará responsável por implementar a fase de extração. O grupo responsável pela extração não deve saber a mensagem que foi inserida; deve saber apenas em que sequência os pixels da imagem receberam os bits resultantes da conversão do texto para binário, conforme é esclarecido a seguir.**

Fase de inserção da mensagem secreta (Grupo 1)

- a) O programa deve receber como entrada uma imagem em formato não-compactado (em .bmp, por exemplo) e codificada em escala de cinzas (8 bits por pixel). Exiba, no programa, a imagem lida na entrada.
- b) Além disso, também deve ser uma entrada do programa uma mensagem de texto, a qual corresponderá à mensagem secreta a ser ocultada na imagem.
- c) O programa deve converter o texto indicado para o formato binário, armazenando-o num vetor, por exemplo.
- d) Em seguida, os bits resultantes do texto convertido para binário devem ser usados para substituir cada um dos bits menos significativos dos valores dos pixels da imagem (que também podem ter sido convertidos de decimal para binário).
- e) Salve a imagem resultante da substituição de bits descrita no item “d” e exiba-a em tela.

Obs.: Observe que o número de caracteres do texto deve ser tal que, após a conversão para binário, a mensagem possua, em bits, um comprimento que corresponda, no máximo, a metade do número de pixels da imagem.

Fase de extração da mensagem secreta (Grupo 2)

- a) Nesta fase da técnica de esteganografia, devem ser realizadas as mesmas ações descritas na fase de inserção da mensagem secreta, porém em ordem reversa. Isto é, deve ser elaborado um programa que receba como entrada a imagem com a mensagem secreta embutida e extraia essa mensagem, exibindo-a, ao final do programa, no formato de texto, de maneira que essa seja legível e coincida, naturalmente, com a mensagem originalmente inserida.
-

2) Essa questão ainda é relacionada à esteganografia LSB, descrita na primeira questão. O grupo responsável por essa questão (**Grupo 3**) deve receber do Grupo 1 uma das imagens originais utilizadas em seu experimento (antes da inserção da mensagem secreta), bem como a imagem correspondente, após a inserção da mensagem secreta. O Grupo 3 deve apenas receber as duas imagens, não sabendo qual delas corresponde à imagem original e qual corresponde à imagem com a mensagem secreta.

- a) Utilizando alguma linguagem de programação, deve ser escrito um código que exiba, na forma de imagem, apenas os bits menos significativos de cada uma das imagens recebidas (observe que isso vai resultar numa imagem binária, isto é, numa imagem em que cada pixel ou é preto (se o LSB correspondente for 0) ou é branco (se o LSB correspondente for 1).
 - b) Ao exibir cada uma das imagens e comparar seus aspectos visuais, que particularidade é percebida? A característica em questão pode auxiliar na identificação de qual das duas imagens corresponda à que possui a mensagem secreta embutida? Explique.
 - c) Agora, implemente no programa uma rotina que exiba apenas os bits mais significativos de cada uma das imagens recebidas. Percebe-se alguma diferença visual entre as imagens? O que aconteceria se a mensagem secreta tivesse sido inserida nesses bits (isto é, nos bits mais significativos da versão binária de cada um dos pixels)?
-