[Assignment -2] Constrained Least Squares (10 Marks)

Q1.

Steganography via least norm. In steganography, a secret message is embedded in an image in such a way that the image looks the same, but an accomplice can decode the message. In this exercise we explore a simple approach to steganography that relies on constrained least squares. The secret message is given by a k-vector s with entries that are all either $+1$ or -1 (*i.e.*, it is a Boolean vector). The original image is given by the n-vector x, where n is usually much larger than k. We send (or publish or transmit) the modified message $x + z$, where z is an n-vector of modifications. We would like z to be small, so that the original image x and the modified one $x+z$ look (almost) the same. Our accomplice decodes the message s by multiplying the modified image by a $k \times n$ matrix D, which yields the k-vector $y = D(x + z)$. The message is then decoded as $\hat{s} = \mathbf{sign}(y)$. (We write $\hat{s}$ to show that it is an estimate, and might not be the same as the original.) The matrix D must have linearly independent rows, but otherwise is arbitrary.

(a) *Encoding via least norm.* Let α be a positive constant. We choose z to minimize $\|z\|^2$ subject to $D(x+z) = \alpha s$. (This guarantees that the decoded message is correct, *i.e.*, $\hat{s} = s$.) Give a formula for z in terms of $D^\dagger$, α, and x.

5 Marks

Hint: *Refer Section* ***16.1.1*** in "Introduction to Applied Linear Algebra, S.Boyd " for least norm derivation using Lagrange Multipliers.

(b) Choose an image x of size 512×512 (any meaningful image is fine). Encode the secrete message $s =$ "IIITBangalore" using some appropriate coding scheme for characters using '1' and '-1' (Note that, the final aim of coding is only to retrieve the string back). Choose the entries of D randomly and compute the pseudo inverse $D^{\dagger}$. Find the value of z using constrained least squares method. The modified image $x + z$ may have entries outside the range [0 1]. We replace any negative values in the modified image with zero, and any values greater than one with one. Adjust α such that the original and modified image looks the same, but the secret message is still decoded correctly.

5 Marks

Additional Instructions:

1- For Q1 (a) , you can upload a printed or a handwritten answer.

2. For Q1 (b) code in python and include a report . The report should contain your coding scheme, the input image and modified image .
Use a separate function *Decode_Message* that accepts *the modified input image, random matrix D* and α.
The function should output the secret code s as a string (“IIITBangalore”) . This function will be verified for the right output.