Assignment 4: Steganography - LSB

I Preliminaries

I.1 Laplace filtering

Let $p$ be a gray scale image given by a $(X, Y)$-matrix. The Laplace operator $L$ for a pixel $p(x, y)$ is given by:

$$L(p(x, y)) = p(x + 1, y) + p(x - 1, y) + p(x, y + 1) + p(x, y - 1) - 4p(x, y)$$

Evaluating the above equation at every point $x, y$ gives the “Laplace filtered” image. Since neighboring pixels are likely to have a similar color, we can expect the values of $L(p(x, y))$ to be tightly clustered around zero. If the image was subject to some modifications, say, it embeds a message in some of its redundant parts, this mentioned statistical property will be altered.

I.2 The Blum Blum Shub PRNG

The Blum Blum Shub (B.B.S.)\(^1\) is a pseudorandom number generator proposed in 1986 by Lenore Blum, Manuel Blum and Michael Shub (Blum et al, 1986).

Blum Blum Shub takes the form:

$$x_{n+1} = (x_n)^2 \mod M$$

where $M = pq$ is the product of two large primes $p$ and $q$. At each step of the algorithm, some output is derived from $x_n$; the output is commonly either the bit parity of $x_n$ or one or more of the least significant bits of $x_n$.

The two primes, $p$ and $q$, should both be congruent to 3$(mod4)$ (this guarantees that each quadratic residue has one square root which is also a quadratic residue) and gcd$(\phi(p - 1), \phi(q - 1))$ should be small (this makes the cycle length large).

\(^1\)The source of information provided in this paragraph is Wikipedia
An interesting characteristic of the Blum Blum Shub generator is the possibility to calculate any $x_i$ value directly (via Euler’s Theorem):

$$x_i = \left( x_0^{2^i \mod (p-1)(q-1)} \right) \mod M.$$

II LSB in 8-bit images - Implementation

- Implement the LSB method for 8-bit gray scale images. For those who use maple, there is a package ImageTools for processing images. You may use the Random Interval Method and the Blum, Blum, Shub PRGN seen in class to embed the message bits into the cover.

- Plot the histograms corresponding to the Laplace filtered raw and stego images. Conclude

- Write a program that recovers a text, encoded in ASCII, hidden in an image.