B-it **Winter IPEC 2009**

Lecturer: Laila El Aimani

Assignment 5: Chi-square method

I EzStego

Implement the steganalysis of the EzStego stegosystem seen in class. You may use as a PRNG the Blum Blum Shub scheme described in the previous exercise sheet. Moreover, you should encrypt the message before embedding using a suitable encryption scheme, say the RSA cryptosystem using adequate parameters.

II Chi-square in DCT steganography

The Jsteg stegosystem was designed by Derek Upham. It embeds the message sequentially in the DCT coefficients of a given image:

Input: message, cover image
Output: stego image
while data left to embed do
  get next DCT coefficient from the the cover image
  if DCT $\neq 0$ and DCT $\neq 1$
    get next LSB from message
    replace DCT LSB with message LSB
  end if
  insert DCT into stego image
end while

It is worth noting that DCT LSB refers to the least significant bit of the quantized DCT coefficients of the image.

1. Show that this system is vulnerable to the Chi-square attack.
2. Implement the Chi-square steganalysis of Jsteg in case the embedded message is an RSA encryption of the secret.
3. Niels Provos improves Jsteg by pseudo random embedding the message using a suitable PRNG, say the Blum Blum Shub generator. The resulting system is called **Outguess 0.1**. Show that the Chi square method can be extended to the local distortions of the image.
4. Implement the statistical attack on Outguess 0.1, and derive the conditions that improve the detection rate of a hidden message embedded using this stegosystem.