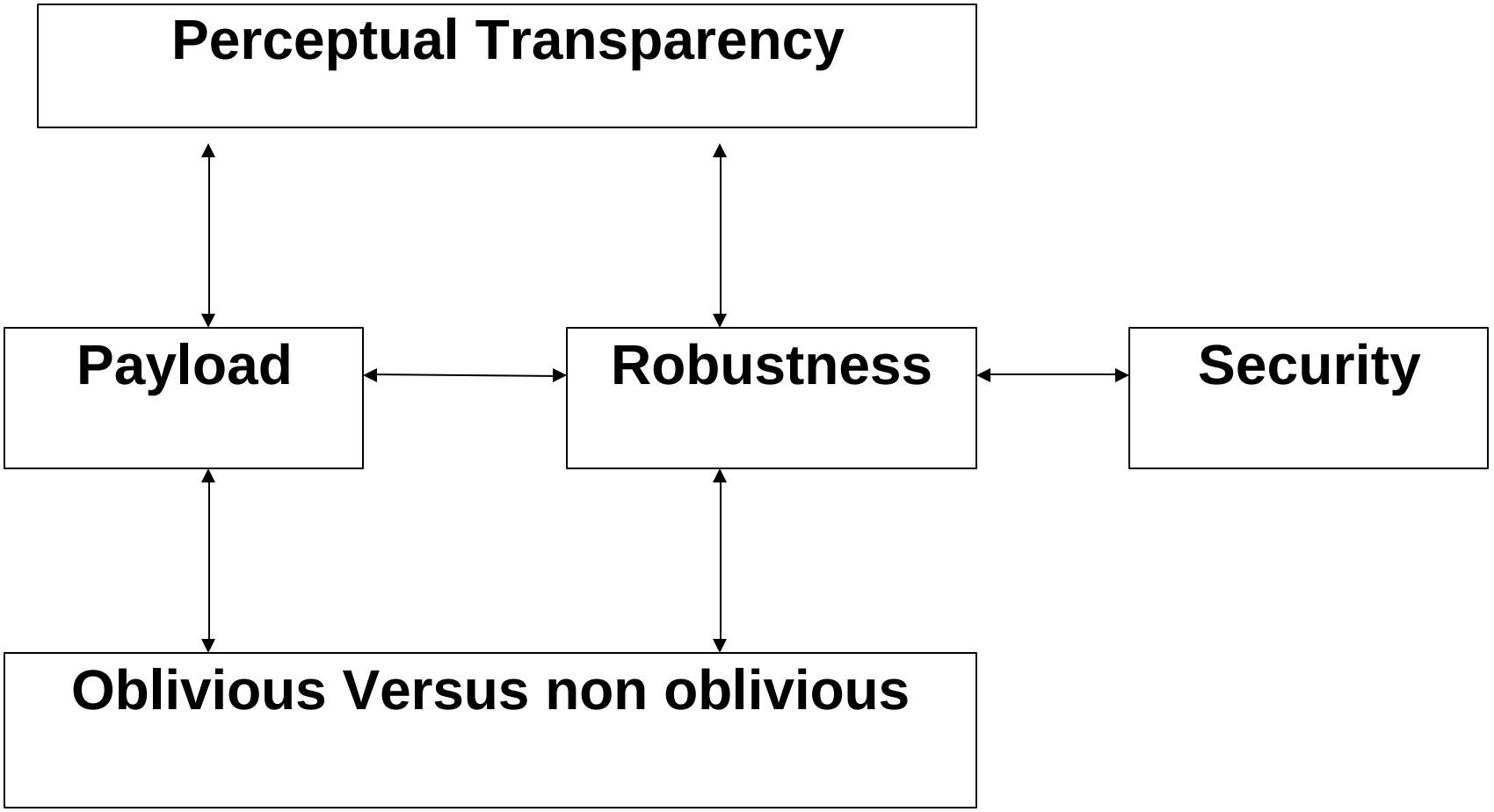
Basic concepts of Digital Watermarking

Prof. Mehul S Raval

Mutual dependencies



Cryptography Vs Steganography

- Cryptography makes messages unintelligible so that those who do not posses secret keys cannot recover the messages.
- Encryption techniques can be used to protect digital data during the transmission from sender to receiver,but Once data is decoded it is not secret.
- Steganography achieve security and privacy by masking the very presence of communication.
- It Complements encryption by embedding the secret imperceptible message which is always present. It’s niche in security is to supplement cryptography and not to replace it.

Spatial Vs Transform Domain Steganography techniques

- In Spatial Domain the watermark is embedded directly into pixels values.
- The image is transformed in transform space like DCT,DFT or DWT prior to watermark embedding and the watermark is hidden in the coefficients representing the image.
- The Watermarked (Stego) image is obtained using an inverse transform.

- Spatial techniques generally adjust lower order bits of image pixel to guarantee imperceptibility
- Cropping or cutting of image portion leads to irretrievable loss of data.
- Eg. LSB Insertion method

- Transform domain allows one to easily place the watermark into significant portion of the image.
- Due to spreading of the data it is less likely to affected.
- The properties of the domain can be explored for improving the various attributes of data hiding.
- Eg:Most Modern techniques are transform domain.

Implementation of Spatial Domain Method(LSB Insertion)

- It is a High bit rate method.
- LSB insertion are that the data can be hidden in the least and second to least bits and still human eye will unable to notice it.
- Consider three pixels represented by three 24 bit words as below

00100111 11101001 11001000

00100111 11001000 11101000

11001000 00100111 11101001

- Inserting ‘A’ (1000001) into three pixel starting from top left byte would result in

(00100111 1110100Æ 1100100∅)

(0010011∅ 1100100∅ 1110100∅)

(11001001 00100111 11101001)

- The emphasized bits are only bits that actually changed.

Implementation of LSB insertion method for Gray scale and Colour Image

- Algorithm Splits the image into 8 planes from MSB to LSB.
- Plane Text encoding is done by converting the Individual character to ASCII value.
- The Message (Text/Binary Image) can be replaced into the LSB plane of the image.
- For Color image is separated into three channels “R”, “G”, “B” and each can be used for encoding so Capacity is thrice the Gray scale image

Experimentation of LSB Insertion Method

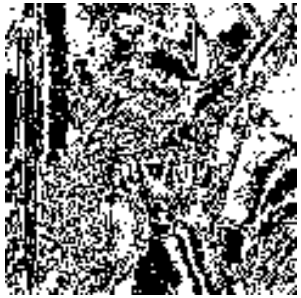
Bit Plane Slicing

MSB of the Image

Second plane

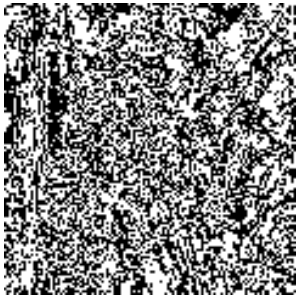
Third plane

Fourth plane

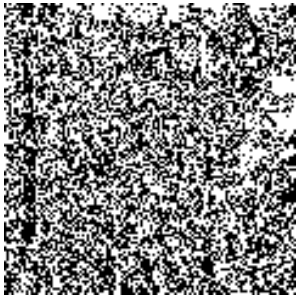


This Plane Contains Minimal Information

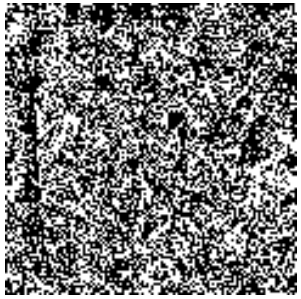
Fifth plane



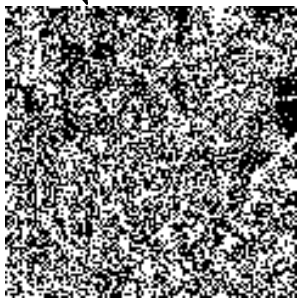
Sixth plane



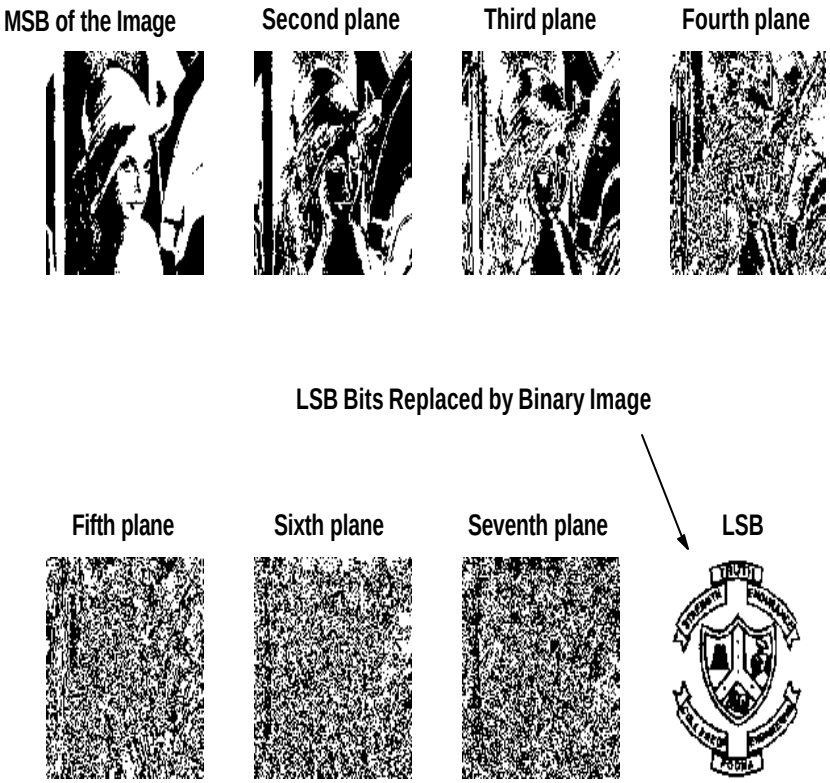
Seventh plane

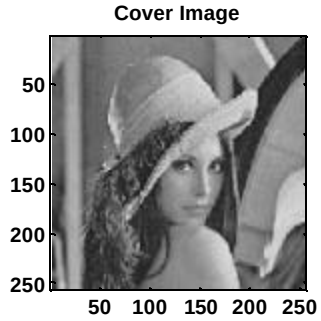


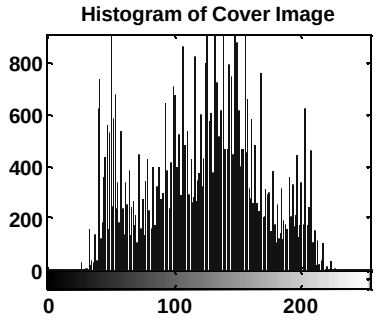
LSB

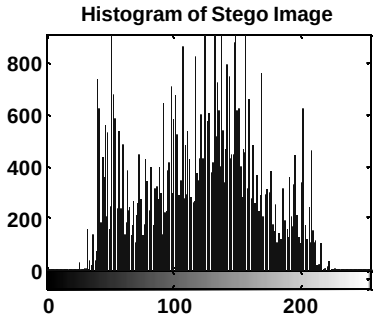


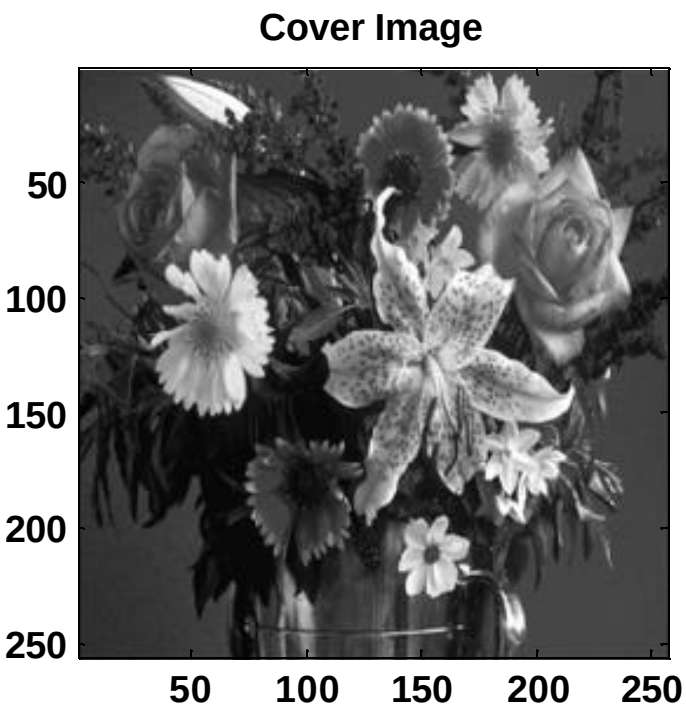
Cover and Stego image for LSB Substitution

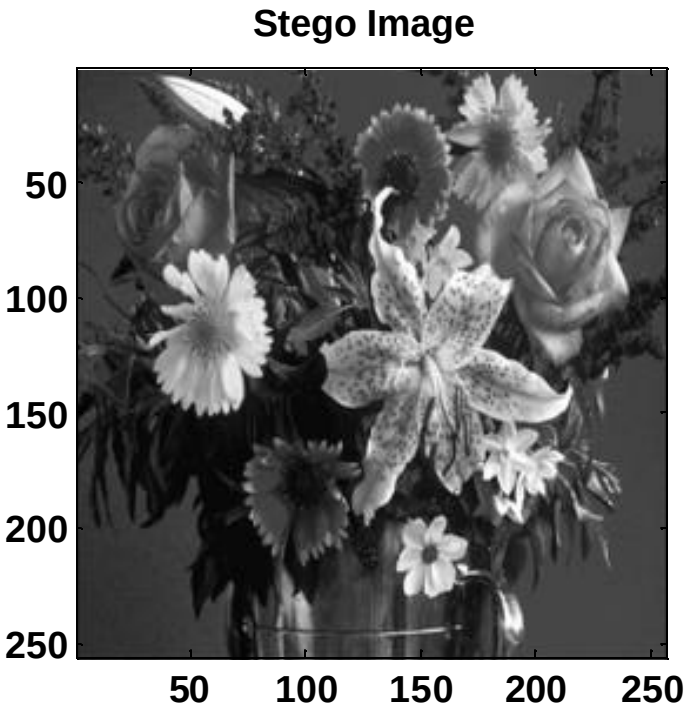








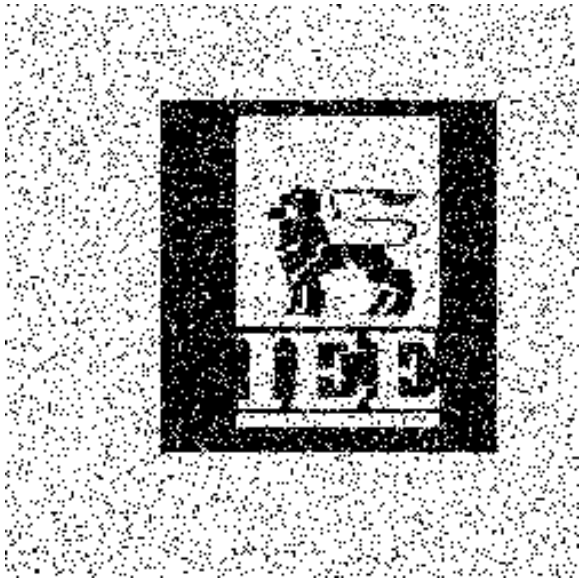

Cover Image
50
100
150
200
250
50
100
150
200
250


Stego Image
50
100
150
200
250
50
100
150
200
250

Stego image subjected to JPEG compression with Q=100

Original Message

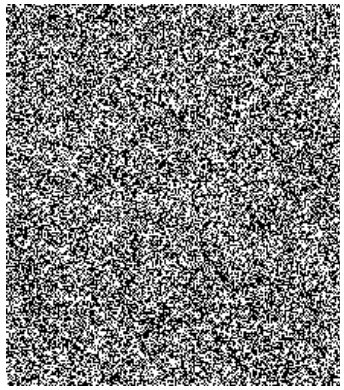
Recovered Message



Stego Image subjected to Gaussian & salt and pepper noise

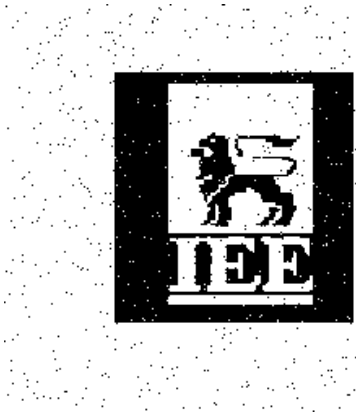
Original Message

Recovered Message



Original Image

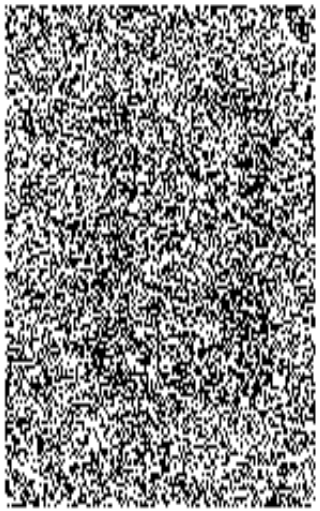
Recovered Image



Stego image subjected to average filtering & cropping

Original Embedded Imformation

Recovered Informatio



Original Embedded Imformation

Recovered Information

Observations and Results

- The LSB plane and plane next to LSB contains practically no visually significant information.
- LSB manipulation gives an enormous amount of capacity in LSB plane for hiding the information.
- This technique is not very secure.
- Hidden information is affected when simple conversion format change from GIF or BMP format to lossy compression format such as JPEG is done, subjected to Guassian noise, Cropping of the stego image.