UNIVERSITY AT ALBANY
State University of New York

DEPARTMENT OF COMPUTER SCIENCE

ICSI-433/533 Theory and Practice of Multimedia Computing – Fall 2019

Homework 4

Due date/time: December 8, 2019, 11:59 p.m. **Total marks: 15**

Late submissions would have penalty 10% every day up to five days.

Objective

The purpose of this assignment is to solidify concepts of image sharing schemes and homomorphic property of Shamir's secret sharing (SSS).

Problems

Question 1

You are given the code for (*k*, *n*) SSS scheme (both share preparation and reconstruction). Extend the implementation of (*k*, *n*) SSS to work for images. You need to show the working of your program by creating shares of an image and show the image shares and the reconstructed image as output. You need to operate on image data, leaving the header intact. You can use any BMP image of your choice. Note that the header length in BMP file format is 54 bytes.

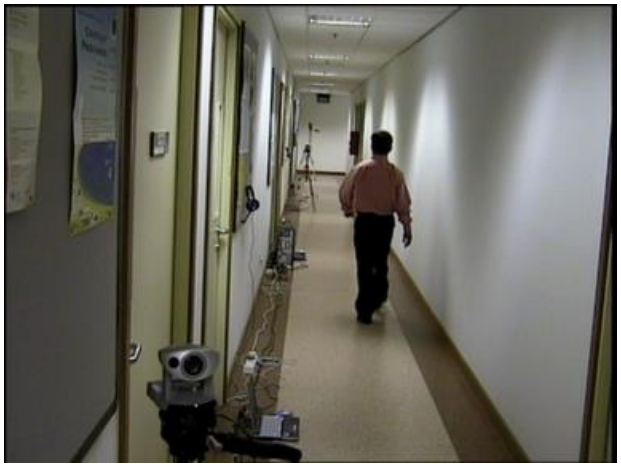
[6 marks]

Question 2

You are required to demonstrate the homomorphic properties of SSS scheme using the image subtraction operation. In a homomorphic encryption scheme, computations performed on encrypted data, when decrypted, generates the same value as when the same computations are performed on the plaintext.

The image subtraction operation takes in two images as input, performs pixel subtraction to create a new image with the absolute value of the difference between pixels of the two input images. You are given a pair of images: a background image and an image with the same background and an object (foreground image). Perform image subtraction on the plain images, then perform image subtraction on the shares of the background and foreground images and reconstruct an image from the result of the subtraction operations. Report your results and observations. Following is an example of a background and foreground image:


background.bmp


foreground.bmp

You are also required to prepare a similar dataset of two images: one background and one foreground and perform all the above operations and report your results and observations.

[9 marks]

Bonus Question (5 marks)

You are required to use the images given to compute their average and demonstrate the homomorphic properties of the average operation. You also need to and prepare a dataset of two images where the foreground object is at different positions in the image and report your results and observations. An example of two such images is as follows:


foreground2.bmp


foreground.bmp

Submission

You must submit the following via UAlbany Blackboard:

(a) Source code along with the instructions to run it.
(b) A pdf file containing your output of Questions 1, 2 & bonus and answers to Question 2 and bonus question.
(c) A pdf file containing your code for Question 1, 2 and bonus.
(d) A video (of max 5 minutes) that shows the working of your program.