Department of Computer Science and Engineering, S V N I T, Surat
End Semester Examination, December 2021
M.Tech.-I Computer Engineering (First Semester)
Course: (CO611) Computer Vision and Image Processing

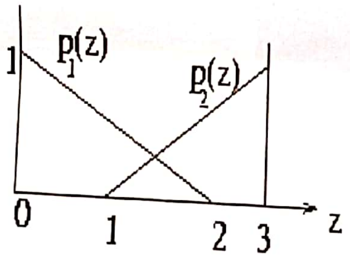
Date: 23 Dec 2021
Time: 9:30 am to 12:30 pm
Marks: 50

Instructions:

1. Write your MTech Admission No/Roll No and other details clearly on the answer books.
2. Assume any necessary data but give proper justifications.
3. Be precise and clear in answering the questions.

Q.1 [10]

(a) Suppose that an image has the gray-level probability density functions shown. Here, $p_1(z)$ corresponds to objects and $p_2(z)$ corresponds to the background. Assume that $P_1 = P_2$ and find the optimal threshold between object and background pixels. [5]



(b) Derive the depth map of a sphere in the form of reflectance map. [2]

(c) What is albedo? How the albedo can be estimated? [1]

(d) What is the charateristic of Lambertian surface? Derive the value of BRDF for it. [2]

Q.2 Answer the following. [16]

(a) Describe the basic block diagram of MPEG encoder and decoder. [4]

(b) Explain the inttraframe and interframe encoding. [4]

(c) Define optical flow. What is an aperature problem? Derive the equations for determining the discrete value of optical flow parameters using calculus of variations technique. [6]

Q.3 Answer the following. [10]

(a) What is MRF? Explain various problems: depth evaluation, image restoration, image de-noising and edge detection as labelling problem in detail. [5]

(b) What is a clique? Explain the energy function and potential function with necessary equations for image segmentation problem using MRF based modelling. [5]

Q.4 Answer any two. [8]

(a) What is an expression for weighted averaging filter of size $m \times n$? Using this expression state the output for the following image segment and filter mask.

Image segment

10	20	30
25	15	35
65	45	55

Filter mask

1	2	1
2	4	2
1	2	1

(b) What is Histogram equalization? What is the transformation function to obtain the histogram equalized image if the histogram of input images is modeled as Gaussian probability density functions of the form

$$p_r(r) = \frac{1}{\sqrt{2\pi}\sigma} \exp - \frac{(r-m)^2}{2\sigma^2}$$

where m and σ are the mean and standard deviation of the Gaussian PDF. The approach is to let m and σ be measures of average gray level and contrast of a given image.

(c) Describe Laplacian and Gradient filters and state the output using each filter for the image segment given in Q.4 (a).

(d) Describe the camera calibration parameters with necessary equations. How these parameters are determined?

Q.5 What is a characteristic curve? Derive the necessary equations to compute changes in $(p.q)$ and z along the characteristic strip for an image irradiance $E(x,y) = f(p^2 + q^2)$. [6]

Department of Computer Science and Engineering, SVNIT, Surat
Endsemester Exam-M.Tech. I (Semester I)
Subject: CO605-Introduction to Computer Security
December 22, 2021
Time: 9:30 am to 12:30 pm, Maximum Marks: 50

Instructions:

The exam is open notes exam. Students can carry handwritten notes (two pages back and forth) with them in exam hall. Attempt any 10 questions. Each question carry 5 marks.

1. For the collision resistant attack on hash function, an adversary wishes to find two messages or data blocks, x and y, that yield the same hash function: $H(x) = H(y)$. This turns out to require considerably less effort than a preimage or second preimage attack. Explain the efforts required by the adversary.

2. The RSA cryptosystem has the following multiplicative property:
$E(m_1).E(m_2) = E(m_1.m_2)$
Explain how this property can be exploited to carry out Existential Forgery in RSA based digital signature schemes. What is the common defense to this attack ?

3. (a) Differentiate Session and Connection in SSL protocol. Explain the advantage of separating session from a connection in SSL.
(b) Which Key Exchange, Signature, Encryption, Block cipher mode of operation and Hash algorithm are used in following TLS cipher suite :
TLS_DHE_DSS_WITH_3DES_EDE_CBC_SHA

4. Alice uses Bob's RSA public key ($e = 7, n = 143$) to send the plaintext P=8 encrypted as ciphertext C=57. Show how Eve can use the chosen ciphertext attack if she has access to Bob's computer to find the plaintext.

5. Briefly explain the idea behind Elliptic curve Cryptography.
   (a) What is the one-way function in this system?
   (b) Define public and private keys in this system.
   (c) Describe the security of this system.

6. Differentiate the following sets with example: $Z, Z_n, Z_{n^*}, Z_p, Z_{p^*}$

7. (a) Discuss the weakness of Data Encryption Standard in today's time. What variants of DES are used to overcome this weakness?
   (b) Compare DES and AES. Which one is bit-oriented? Which one is byte-oriented?

8. What is the disadvantage of Electronic Code Book Mode of operation for block ciphers? Discuss any one mode of operation which overcome this disadvantage.

9. Solve the simultaneous congruences:
x ≡ 6 mod 11 , x ≡ 13 mod 16, x ≡ 9 mod 21, x ≡ 19 mod 25

10. "When the hash of the message is signed instead of the message itself, the susceptibility of the RSA digital signature scheme depends on the strength of the hash algorithm." Justify the statement with suitable arguments.

11. Discuss Man-in-the-Middle attack in Diffie-Hellman key agreement protocol. Suggest the solution that can overcome this attack.

12. Consider an elliptic curve $y^2 = x^3 + 2x + 2 \bmod 17$. Given a base point P=(5,1), Calculate 3P.