REG.NO.:

SLOT:F2+TF2

Vellore Institute of Technology
(Deemed to be University under section 3 of UGC Act, 1956)

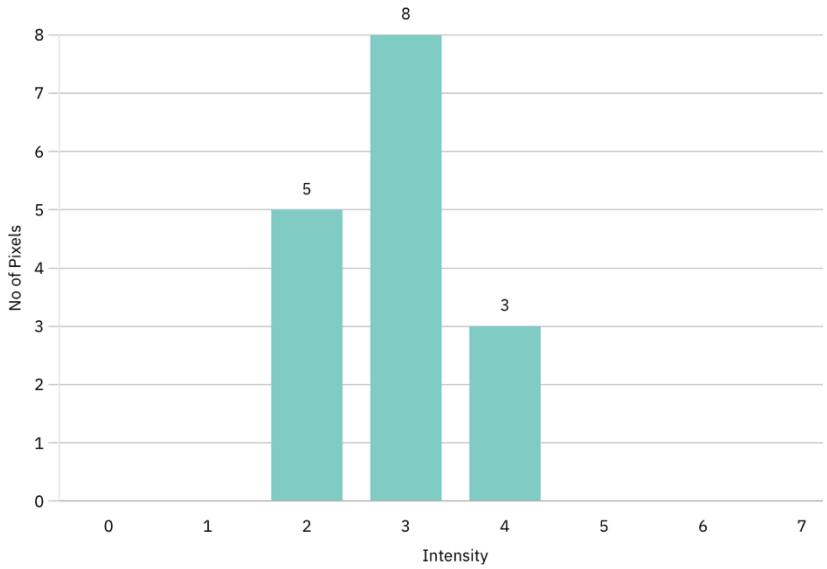
SCHOOL OF COMPUTER SCIENCE AND ENGINEERING
CONTINUOUS ASSESSMENT TEST - II
FALL SEMESTER 2025-2026

BCSE323L- Digital Watermarking and Steganography
Answer Key

Q. No	Question	Marks
1.	A game studio decides to protect its retro pixel-art game from piracy by embedding a secret binary watermark into the character sprites. The sprites are stored as 4×4 grayscale images, with pixel intensities ranging from 0 to 7. A sample sprite is given in S. $$S = \begin{bmatrix} 2 & 3 & 3 & 4 \\ 3 & 2 & 4 & 3 \\ 2 & 3 & 3 & 2 \\ 4 & 3 & 2 & 3 \end{bmatrix}$$ a) Plot the histogram of the sprite's pixel values and identify the peak point and a suitable zero point for embedding. b) Demonstrate how the watermark sequence [1, 0, 1, 0] is embedded using histogram shifting into S. c) Explain how the studio could remove the watermark and recover the original sprite, ensuring no visual distortion in the pixel art.	(3 + 4 + 3)

Answer:

a)



Peak point – p = 3
Zero point – z = 5

b) m=1010
pixels with value 4 is replaced by 5
8 pixels with intensity=3.

SCHOOL OF COMPUTER SCIENCE AND ENGINEERING
CONTINUOUS ASSESSMENT TEST - II
FALL SEMESTER 2025-2026

$$S = \begin{bmatrix} 2 & 4 & 3 & 5 \\ 4 & 2 & 5 & 3 \\ 2 & 3 & 3 & 2 \\ 5 & 3 & 2 & 3 \end{bmatrix}$$

c)removal: Receiver knows p=3 and z=5 and scans the same positions in the same order.

- If value = p (3) → extracted bit = 0; restore pixel to 3.
- If value = p+1 (4) → extracted bit = 1; restore pixel to 3.
- (Other values are ignored for these positions.)

Finally replace all 5s by 4

$$output = \begin{bmatrix} 2 & 3 & 3 & 4 \\ 3 & 2 & 4 & 3 \\ 2 & 3 & 3 & 2 \\ 4 & 3 & 2 & 3 \end{bmatrix}$$

2. A messaging app wants to secure its sensitive unreleased text campaigns before sending them to beta testers. The app needs to ensure that even a single-character change in a text message is detectable, that the security measures remain intact despite common text transformations like copying into a different platform or changing font encoding, and that premium testers can restore the exact original message after verification. Name the different methods that can be used to secure text messages, and describe the drawbacks of each method. How should the app combine or adapt these methods to guarantee authenticity, prevent forgery, and still allow original restoration without triggering false positives? — 10

Answer: Exact authentication

Methods –

1. Fragile Watermarks – drawbacks:

- Easily forged: If the watermark is not dependent on the cover work's actual content
- Overly sensitive: Even benign modifications (format conversion, compression, or metadata changes) can destroy the watermark and cause false positives.
- Limited authentication: Can only indicate *that* a change occurred not *where* or *how*.

2. Embedded Signatures - drawbacks:

- Difficult to remove: Makes exact restoration of the original work impossible.
- Increased distortion risk: Embedding a robust watermark may slightly degrade the original media.

3. Erasable Watermarks- drawbacks:

- Complex design: Constructing a perfectly erasable watermark without residual artifacts is challenging.
- Security risk: If the erasure key or algorithm is leaked, attackers could remove or replace the watermark.
- Extra computation: Embedding, erasing, and verifying all require additional processing steps.

Can combine as follows:

1. **Embedder:**
   - Compute a cryptographic hash of the original work.
   - Sign it with a private key.
   - Embed this signature using an **erasable fragile watermark**.
2. **Receiver:**
   - Extract and verify the embedded signature.
   - Erase the watermark to restore the original.
   - Recompute the hash of the restored work and compare it to the extracted one.

If hashes match; Work is authentic.
If not; Work has been modified.

---

3. An image security analyst is asked to hide a secret message inside a JPEG image before transmitting it over a network. The quantized DCT coefficients of one image block are stored in the matrix Q. (5 + 5)

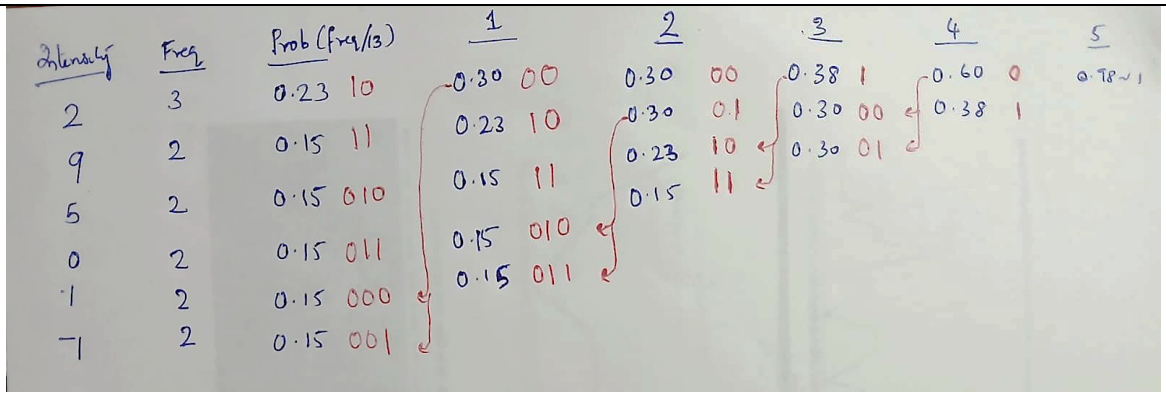
$$Q = \begin{bmatrix} 9 & 3 & 8 & 3 & 0 & 0 & 0 & 0 \\ 4 & 1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 2 & 0 & 0 & 0 & 0 & 0 \\ 5 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ -1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}$$

a) Find the embedding capacity of the block. Generate the zig-zag sequence from Q and embed the secret message [0, 1, 1, 0, 1] after truncating the trailing zeroes.
b) Illustrate how the modified sequence is compressed and encoded for transmission using Huffman coding.

Answer:
a) Embedding capacity = 6
Zig zag sequence: 9 **3 4** 0 1 **8 3** 1 0 **5** -1 1 **2** 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
Truncate trailing 0s: 9 **3 4** 0 1 **8 3** 1 0 **5** -1 1 **2**
LSB embedding [0, 1, 1, 0, 1] to AC components only (other than 0,1, -1):
9 2 5 0 1 9 2 1 0 5 -1 1 2
b) Huffman coding on 9 2 5 0 1 9 2 1 0 5 -1 1 2

Vellore Institute of Technology
(Deemed to be University under section 3 of UGC Act, 1956)

SCHOOL OF COMPUTER SCIENCE AND ENGINEERING
CONTINUOUS ASSESSMENT TEST - II
FALL SEMESTER 2025-2026

	 9 2 5 0 1 9 2 1 0 5 -1 1 2 is encoded as 1110010011000111000001101000100010	
4.	A streaming company wants to embed secret tracking codes into its audio files before releasing them to different platforms. The system must be robust to common processing, remain imperceptible to listeners without noticeable loss of audio quality, and be difficult for attackers to detect or remove. As an engineer, evaluate sequential embedding, selective embedding, and frequency masking with amplitude thresholding in terms of embedding capacity, robustness against attacks, detectability, and audio quality. Which approach/combination would you recommend and why? Answer: • **Sequential embedding:** High capacity but low robustness; easily detected and degraded by compression or filtering; noticeable artifacts reduce audio quality. • **Selective embedding:** Moderate capacity; good robustness when embedding only in stable, high-energy regions; less detectable and maintains better quality. • **Frequency masking + amplitude thresholding:** Lower capacity but highest imperceptibility and robustness; hides watermark under psychoacoustic masking so it survives compression and remains inaudible. **Recommendation:** Use **selective embedding guided by frequency-masking with amplitude thresholding**. This ensures: • High audio quality (imperceptible changes). • Strong robustness to common processing. • Low detectability and resistance to removal.	10
5.	A researcher is using a ternary Hamming code system with ± 1 embedding to embed the secret data D=[1,1,2] in a grayscale image G using the parity-check matrix H. Compute the syndrome and prove that the covering radius is 1. Finally display the stego output image.	10

$$G = \begin{bmatrix} 50 & 51 & 59 & 53 \\ 52 & 53 & 58 & 57 \\ 46 & 47 & 40 & 45 \\ 49 & 50 & 59 & 42 \end{bmatrix}$$

$$H = \begin{bmatrix} 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 2 & 1 & 2 & 0 \\ 1 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 2 & 1 & 2 & 0 & 1 \\ 1 & 0 & 1 & 1 & 1 & 0 & 0 & 2 & 1 & 1 & 0 & 1 & 2 \end{bmatrix}$$

Answer:

Message length, p =3; ternary hamming code=> q=3

number of cover pixels needed is $\frac{q^p-1}{q-1} = \frac{3^3-1}{2}$=13.

Take the first 13 pixels from G in row-major order

g = [50, 51, 59, 53, 52, 53, 58, 57, 46, 47, 40, 45, 49]

x =g mod 3 = [2, 0, 2, 2, 1, 2, 1, 0, 1, 2, 1, 0, 1]

$$\text{Syndrome} = Hx \bmod 3 = \begin{bmatrix} 2+0+2+0+0+0+1+0+1+4+1+0+0 \\ 2+0+0+2+0+2+0+0+2+2+2+0+1 \\ 2+0+2+2+1+0+0+0+1+2+0+0+2 \end{bmatrix}$$

$$= \begin{bmatrix} 11 \\ 13 \\ 12 \end{bmatrix} mod\ 3 = \begin{bmatrix} 2 \\ 1 \\ 0 \end{bmatrix}$$

Given H is a [13, 10] code with covering radius R = 1. The radius is 1 because we need only a linear combination of one column to obtain any syndrome. For example, the syndrome (2, 2, 2) , which does not appear directly as a column in H, can be obtained as a linear combination (multiple) of just one column, the seventh column.

$$\text{m-Hx} = \begin{bmatrix} 1 \\ 1 \\ 2 \end{bmatrix} - \begin{bmatrix} 2 \\ 1 \\ 0 \end{bmatrix} \bmod 3 = \begin{bmatrix} 2 \\ 0 \\ 2 \end{bmatrix} = 2*H(3)$$

y[3]=x[3]+2 = 2+2 mod3 = 1

To make g[3] as 1 mod 3; 59-1 = 58.

$$stego\ output\ image = \begin{bmatrix} 50 & 51 & 58 & 53 \\ 52 & 53 & 58 & 57 \\ 46 & 47 & 40 & 45 \\ 49 & 50 & 59 & 42 \end{bmatrix}$$

****