17168

BRAINWARE UNIVERSITY

Term End Examination 2025-2026
Programme – B.Sc.(ANCS)-Hons-2023
Course Name – Digital Watermarking and Steganography
Course Code - BNC50204
(Semester V)

Full Marks : 60 **Time : 2:30 Hours**

[The figure in the margin indicates full marks. Candidates are required to give their answers in their own words as far as practicable.]

Group-A
(Multiple Choice Type Question) 1 x 15=15

1. *Choose the correct alternative from the following :*

(i) Which technique uses both a training set and test set?
- a) Compression algorithms
- b) Blind steganalysis
- c) Data embedding
- d) Error correction

(ii) Which is an essential step in testing steganographic systems?
- a) Avoiding steganalysis tools
- b) Using large and diverse datasets
- c) Only encrypting the message
- d) Reducing cover Work resolution

(iii) Which action should designers take to improve practical security?
- a) Avoid embedding in noisy areas
- b) Use complex mathematical constructs
- c) Reduce cover Work size
- d) Hide larger messages

(iv) Which condition makes a steganographic system practically secure?
- a) It cannot be analyzed by any steganalysis method
- b) It resists both targeted and blind steganalysis
- c) It hides very large messages
- d) It compresses the cover Work

(v) Which scenario involves compressing or downsampling to block hidden messages?
- a) Passive warden
- b) Active warden
- c) Malicious warden
- d) Friendly warden

(vi) How can steganographic security status change suddenly?
- a) By adding more embedding capacity
- b) Due to new steganalysis methods
- c) By increasing compression
- d) By increasing key length

(vii) What is the key difference between a crypto key and a stego key?
- a) Crypto key encrypts the message, stego key controls embedding
- b) Both are used for encryption
- c) Stego key encrypts, crypto key embeds
- d) Both function the same

(viii) Which technique is ideal for embedding in high-noise environments?
- a) LSB watermarking
- b) Spread spectrum watermarking
- c) DCT watermarking
- d) Histogram shifting

(ix) Identify the meaning of informed embedding in watermarking.

a) Embedding without using any prior information
b) Embedding with access to cover signal details
c) Random embedding
d) Blind embedding

(x) Identify where JPEG compression most affects watermarked signals.

a) LSB domain
b) DCT domain
c) Time domain
d) Color space

(xi) Select the meaning of robustness in watermarking.

a) Low computational cost
b) Ability to survive attacks and distortions
c) Reduced bitrate
d) Simplified detection algorithms

(xii) Identify a distortion that histogram-based watermarking can resist.

a) Geometric distortions
b) Volumetric distortions
c) Temporal distortions
d) Synchronization attacks

(xiii) Select the purpose of synchronization patterns in watermarking.

a) Speed up watermark detection
b) Reduce watermark size
c) Align watermarks after temporal distortions
d) Encrypt the watermark

(xiv) Identify the main technique for copyright protection.

a) Fragile watermarking
b) Semi-fragile watermarking
c) Robust watermarking
d) Geometric watermarking

(xv) Identify the term for the original file without hidden data.

a) Stego Object
b) Cover Object
c) Ciphertext
d) Plaintext

Group-B

(Short Answer Type Questions) 3 x 5=15

2. Define the role of a passive warden in steganography. (3)
3. What is Sample Pairs Analysis used for in steganalysis? (3)
4. Define the concept of digital watermarking. (3)
5. Identify the contributor of Dirty-Paper Coding and describe the problem it addresses in watermarking. (3)
6. Define the concept of entropy and evaluate its role in information-theoretic steganography. (3)

OR

Assess the contribution of machine learning techniques to modern steganalysis applications. (3)

Group-C

(Long Answer Type Questions) 5 x 6=30

7. Explain the differences between passive, active, and malicious wardens in steganography with suitable examples. (5)
8. Describe any one hybrid digital watermarking technique and explain how it improves watermark performance. (5)
9. Explain collusion attacks in watermarking. Why are they dangerous, and how can they be mitigated? (5)
10. Analyze in detail the concept of steganography, including its objectives, process, and key terminologies such as cover object, stego object, payload, and stego key. (5)
11. Compare and contrast steganography and cryptography. How can they be combined in hybrid systems for enhanced security in communication? (5)
12. Discuss various robust watermarking approaches. Compare spatial domain, frequency domain, and hybrid watermarking methods with examples. (5)

OR

Analyze the critical security requirements for robust watermarking systems. Identify how encryption and cryptographic key management enhance watermark security. (5)