

Tên học phần:	<u>Ẩn dữ liệu & Chia sẻ thông tin</u>	Mã HP:	<u>CTT321</u>
Thời gian làm bài:	<u>90 phút</u>	Ngày thi:	<u>06/01/2017</u>
Ghi chú: Sinh viên [<input checked="" type="checkbox"/> được phép / <input type="checkbox"/> không được phép] sử dụng tài liệu khi làm bài. Sinh viên làm bài trực tiếp trên đề từ trang 6 Sinh viên nộp cả đề thi và phần trả lời, KHÔNG tách phần đề và phần trả lời ra.			

Mã Đề: 01

Họ & Tên:

MSSV:

PHẦN TRẮC NGHIỆM (7.0 điểm)

Câu 1. Khái niệm nào dưới đây không cùng nhóm với các khái niệm còn lại?

- A. Fingerprinting
- B. Visible watermarking
- C. Imperceptible watermarking
- D. Steganography

Câu 2. Ứng dụng nào dưới đây không phải là ứng dụng của ẩn dữ liệu?

- A. Trao đổi thông tin bí mật
- B. Bảo vệ tác quyền
- C. Hỗ trợ tìm kiếm thông tin
- D. Bảo vệ tính toàn vẹn dữ liệu

Câu 3. Việc che giấu định danh của người gửi/người nhận gọi là gì?

- A. Covert channel
- B. Steganography
- C. Anonymity
- D. Watermarking

Câu 4. Màu C trong hệ màu CMYK đại diện cho màu gì?

- A. Màu tím
- B. Màu xanh lơ
- C. Màu trắng
- D. Độ trong suốt của màu

Câu 5. Kí hiệu M trong bài toán Steganography ám chỉ?

- A. Đối tượng chưa đánh dấu
- B. Đối tượng đã đánh dấu
- C. Thông tin mật
- D. Tín hiệu đã thủy văn

Câu 6. Công thức $I \times I \times K \times W \rightarrow \{0,1\}$ biểu diễn cho?

- A. Quá trình nhúng
- B. Quá trình rút trích
- C. Quá trình gây nhiễu
- D. Tất cả đều đúng

Câu 7. Mỗi điểm ảnh trong ảnh xám được lưu trữ bằng?

- A. 1 bit
- B. 2 bits
- C. 8 bits
- D. 24 bits

Câu 8. LSB là viết tắt của?

- A. Low sample bit
- B. Least significant byte
- C. Large significant bit
- D. Least significant bit

Câu 9. Trong giao thức giấu tin mật sử dụng khóa công khai (public key steganography), khóa công khai được dùng để làm gì?

- A. Nhúng thông điệp mật vào cover.
- B. Trích thông điệp mật từ đối tượng stego.
- C. Mã hóa thông điệp mật
- D. A & B đều đúng

Câu 10. Trong mô hình chia sẻ thông tin của Shamir với $n = 12, k = 7$, cần phát sinh bao nhiêu số ngẫu nhiên để xây dựng hàm đa thức $f(x)$?

- A. 6
- B. 7
- C. 11
- D. 12

Câu 11. Phương pháp nào sau đây không thể phục hồi tín hiệu gốc?

- A. LSB
- B. Patchwork
- C. Dựa trên khác biệt cặp pixel
- D. A & B đều đúng.

Câu 12. Cho 2 điểm ảnh có giá trị lần lượt là 103 và 98, sử dụng phương pháp nhúng dựa trên khác biệt cặp pixel để nhúng bit 1 vào 2 điểm ảnh này. Giá trị của 2 điểm ảnh sau khi nhúng là?

- A. $x' = 96, y' = 104$
- B. $x' = 96, y' = 105$
- C. $x' = 95, y' = 106$
- D. $x' = 106, y' = 95$

Câu 13. Cho 2 điểm ảnh có giá trị lần lượt là 98 và 103, sử dụng phương pháp nhúng dựa trên khác biệt cặp pixel để

nhúng bit 1 vào 2 điểm ảnh này. Giá trị của 2 điểm ảnh sau khi nhúng là?

- A. $x' = 96, y' = 104$
- B. $x' = 96, y' = 105$
- C. $x' = 95, y' = 106$
- D. $x' = 106, y' = 95$

Câu 14. Sau khi áp dụng DFT lên tín hiệu S gồm N mẫu, người ta thu được một thành phần DFT $F[k] = i3 + 4$. Hãy cho biết giá trị amplitude và phase của thành phần DFT nói trên?

- A. $A = 3, \theta = 4$
- B. $A = 4, \theta = 3$
- C. $A = 4, \theta = 1.570$
- D. $A = 5, \theta = 0.643$

Câu 15. Phát biểu nào sau đây là sai?

- A. Stego key được dùng để chọn các thành phần cover để nhúng trong phương pháp LSB.
- B. Các thành phần tương ứng với tần số thấp là thành phần ít quan trọng của ảnh.
- C. Nhúng thông điệp mật trong miền DCT cho phép ảnh nhúng chịu được tấn công nén JPEG.
- D. Hệ số DCT là số thực, trong khi DFT là số phức.

Câu 16. An sử dụng thuật toán Patchwork mở rộng để nhúng thủy vân "101" vào tấm ảnh như hình bên dưới. Giả sử An dùng khóa bí mật và phát sinh được các cặp điểm ảnh như sau:

$$a_i = \{(0, 2), (1, 3), (2, 4)\}$$

$$b_i = \{(2, 1), (3, 3), (3, 2)\}$$

18	13	21	26	23
----	----	----	----	----

21	1	32	5	42
5	9	9	21	17
10	39	18	43	43
0	8	15	1	11

Cho biết có bao nhiêu điểm ảnh bị thay đổi giá trị sau khi thực hiện nhúng watermark?

- A. 0
- B. 2
- C. 4
- D. 6

Câu 17. Với cùng giả thuyết được cho ở Câu 16 cho biết giá trị của điểm ảnh ở vị trí (2, 4) sau quá trình nhúng là bao nhiêu?

- A. 5
- B. 15
- C. 21
- D. 32

Câu 18. Với cùng giả thuyết cho ở Câu 16, cho biết giá trị PSNR của ảnh trước và sau khi nhúng là bao nhiêu?

- A. 29.99366
- B. 30.26329
- C. 42.19794
- D. Không xác định

Câu 19. Phép biến đổi nào sau đây cho phép thông tin nhúng không bị ảnh hưởng bởi phép dịch chuyển hình học (translation)?

- A. DFT
- B. Mellin Fourier
- C. A và B đều sai
- D. A và B đều đúng

Câu 20. Với phương pháp trải phổ Direct – sequence, tín hiệu thủy văn sau khi lấy mẫu nhiều lần được trộn với tín hiệu nhiễu giả ở băng tần rộng bằng phép gì?

- A. OR
- B. AND
- C. XOR
- D. A, B & C đều sai.

Câu 21. Với không gian màu YIQ, người ta thường dùng kênh nào để nhúng thủy văn để đảm bảo tính vô hình (invisible) của thủy văn?

- A. Y
- B. I
- C. Q
- D. Cả 3 kênh đều được.

Câu 22. Kỹ thuật nào dưới đây được dùng để thay đổi định dạng watermark trước khi nhúng nó vào cover?

- A. Trải phổ
- B. Iteration Mapping
- C. A và B đều sai
- D. A và B đều đúng

Câu 23. Để đảm bảo tính bất biến với phép quay (rotate) và tỉ lệ (scale), phép biến đổi Mellin đã làm gì?

- A. Áp dụng LPM cho thành phần Amplitude của DFT lần 1
- B. Áp dụng LPM cho thành phần Amplitude của DFT lần 2
- C. Áp dụng LPM cho thành phần Phase của DFT lần 1
- D. Áp dụng LPM cho thành phần Phase của DFT lần 2.

Câu 24. Cho tám ảnh sau khi nhúng thông điệp mật bằng phương pháp vùng

cover và bit đồng nhất dưới đây. Biết rằng mỗi vùng có kích thước là 3×3 cho biết bit được nhúng ở vùng thứ nhất và thứ 2 là bao nhiêu?

23	28	0	34	26	27
14	44	17	49	5	115
31	7	29	33	23	74
44	16	16	34	21	166
20	24	33	4	14	107

- A. 00
B. 01
C. 10
D. 11

Câu 25. Cho một khối ảnh từ một tấm ảnh nhị phân thu được sau quá trình nhúng thông điệp mật bằng thuật toán Zhao & Koch. Cho biết phần trăm điểm ảnh trắng trong khối ảnh đã cho?

1	0	1	0	1	1	0	0
0	1	1	0	1	1	0	1
0	0	1	0	0	0	1	0
0	0	0	1	0	1	1	1
1	1	0	0	0	0	0	1
0	0	1	1	0	1	0	0
0	0	1	0	0	1	0	1
1	1	1	0	0	0	0	1

- A. 43.75%
B. 56.25%
C. 34.75%
D. 65.25%

Câu 26. Với cùng giả thuyết cho ở Câu 25. Biết rằng ngưỡng $R_0 = 48, R_1 = 52, \lambda = 2\%$, cho biết bit được nhúng trong khối ảnh đã cho là gì?

- A. 0
B. 1
C. 2
D. Không có giá trị nhúng

Câu 27. Với cùng giả thuyết cho ở Câu 25. Biết rằng ngưỡng $R_0 = 48.5, R_1 = 51.5, \lambda = 1.5\%$, cho biết bit được nhúng trong khối ảnh đã cho là gì?

- A. 0
B. 1
C. 2
D. Không có giá trị nhúng

Câu 28. Phát biểu nào sau đây là đúng?

- A. Phương pháp nhúng thủy vân càng mạnh (robust) thì tính vô hình (invisble) của thủy vân càng cao.
B. Giá trị FP trong phương pháp đánh giá ROC cho biết số ảnh bị nhận nhầm là có thủy vân.
C. Đầu ra của một quá trình rút trích thủy vân là một thủy vân.
D. Bit-error rate cho biết tính vô hình của của thủy vân số

Câu 29. An sử dụng mô hình chia sẻ ảnh nhị phân $(2, 2)$ cho ảnh nhị phân $A = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 1 & 1 & 1 \end{bmatrix}$. Biết rằng các ma trận B_i được phát sinh ngẫu nhiên như sau:

$$B_1 = \begin{bmatrix} 0 & 1 & 1 \\ 1 & 0 & 0 \\ 1 & 1 & 1 \end{bmatrix}, B_2 = \begin{bmatrix} 0 & 0 & 1 \\ 0 & 0 & 0 \\ 0 & 1 & 1 \end{bmatrix},$$

$$B_3 = \begin{bmatrix} 0 & 1 & 1 \\ 1 & 0 & 0 \\ 1 & 0 & 0 \end{bmatrix}$$

Cho biết shadow thứ $i = 1$ là gì?

A. $A'_1 = \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 1 & 1 & 1 \end{bmatrix}$

B. $A'_1 = \begin{bmatrix} 0 & 1 & 1 \\ 0 & 0 & 0 \\ 1 & 1 & 1 \end{bmatrix}$

C. $A'_1 = \begin{bmatrix} 0 & 1 & 1 \\ 1 & 0 & 0 \\ 1 & 0 & 0 \end{bmatrix}$

D. $A'_1 = \begin{bmatrix} 0 & 1 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 1 \end{bmatrix}$

Câu 30. Giả sử An sử dụng mô hình Noir và Shamir để chia sẻ ảnh nhị phân với phép chia $(3, n), n = 4$. Cho biết số pixel mở rộng cho mỗi pixel của ảnh mật và độ tương phản tương đối tương ứng là bao nhiêu?

A. $m = 2, \alpha = \frac{1}{2}$

B. $m = 4, \alpha = \frac{1}{4}$

C. $m = 6, \alpha = \frac{1}{6}$

D. $m = 8, \alpha = \frac{1}{8}$

Câu 31. Với cùng giả thuyết của Câu 30, cho biết ma trận BI tương ứng là gì?

PHẦN TỰ LUẬN (3.0 điểm)

Câu 1 (1.5 điểm).

An sử dụng mô hình Shamir với $n = 5, k = 3, P = 211$ để chia sẻ thông tin mật. Ba người tham gia P_1, P_2 và P_3 lần lượt giữ các shadow $(1, 171), (2, 46)$, và $(3, 170)$ muốn khôi phục lại thông tin mật mà An đã chia sẻ. Sinh viên hãy chỉ ra chi tiết các bước tính và cho biết thông tin mật mà An đã chia sẻ là gì?

Câu 2 (1.5 điểm).

Liệt kê 3 chủ đề đã được trình bày bởi các nhóm trong đồ án tìm hiểu. Sinh viên cần ghi tóm tắt nội dung cho từng chủ đề.

----- Chúc các bạn làm bài tốt -----

A. $BI = \begin{bmatrix} 1 & 1 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}$

B. $BI = \begin{bmatrix} 1 & 1 & 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 0 & 1 \end{bmatrix}$

C. $BI = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 \end{bmatrix}$

D. $BI = \begin{bmatrix} 1 & 1 & 0 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 0 & 1 & 1 \end{bmatrix}$

Câu 32. Với cùng giả thuyết Câu 30. Biết rằng hoán vị sử dụng là $\{3, 4, 5, 2, 6, 1\}$, cho biết ma trận nào sau đây dùng để chia sẻ điểm ảnh trắng?

A. $\begin{bmatrix} 1 & 0 & 0 \\ 1 & 0 & 1 \end{bmatrix}$

B. $\begin{bmatrix} 1 & 1 & 1 \\ 0 & 1 & 0 \end{bmatrix}$

C. $\begin{bmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \end{bmatrix}$

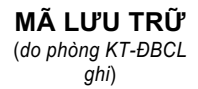
D. $\begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix}$

PHẦN TRẢ LỜI TRẮC NGHIỆM

Lưu ý:

- Để chọn câu trả lời, sinh viên **tô đậm** lựa chọn.
- Để bỏ lựa chọn, sinh viên **đánh dấu chéo** vào lựa chọn
- Để chọn lại, sinh viên **khoanh tròn** lựa chọn

Câu	A	B	C	D	Câu	A	B	C	D
1	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	17	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
2	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	18	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
3	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	19	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
4	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	20	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
5	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	21	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
6	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	22	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
7	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	23	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
8	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	24	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
9	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	25	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
10	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	26	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
11	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	27	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
12	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	28	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
13	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	29	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
14	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	30	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
15	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	31	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
16	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	32	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>



[illegible]