**BÀI TẬP**

1. Cho ma trận ảnh lượng tử như sau, hãy mã hóa thành mã nhị phân theo phương pháp nén ảnh JPEG biết giá trị DC của khối DCT trước là 46.

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 134 | 12 | -3 | 0 | 0 | 0 | 0 | 0 |
| 5 | 0 | 4 | 0 | 0 | 0 | 0 | 0 |
| 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| -25 | -9 | 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 |

**Giải**:

Quét zigzac:

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 88 | 12 | 5 | 0 | 0 | -3 | 0 | 4 |
| 0 | 0 | -25 | 0 | 0 | 0 | 0 | 0 |
| 0 | 0 | 0 | -9 | 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 |

88, (0,12),(0,5),(2,-3),(1,4),(2,25),(8,-9),EOB

Delta= 134-46=88

->loại delta= 2^6<=88<2^7 ->loại delta =7

Tra bảng Huffman: phần 1:11110

Phần 2: 88= 1011000

* Phần DC là **11110 1011000**

(0,12) thuộc loại 4 -> phần 1 có:1011 tổng độ dài 8bit

Phần 2 : 1100 -> mã vlc của rlc là :**1011 1100**

(0,5) thuộc loại 3 -> phần 1:100 tổng 6bit

Phần 2 :101 -> mã vlc của rlc là:**100 101**

(2-3)->loại 2-> phần 1 có:01 độ dài 4bit

Phần 2: biên độ: 2^2-3-1=0 -> phần 2:00 -> tổng độ dài :**0100**

(1,4): loại 3 Phần 1:1111001 tổng độ dài là 10

Phần 2:100 tổng độ dài vlc của rlc là:**1111001 100**

(2,25): loại 5 : phần 1:1111 1111 1000 1010 độ dài 21

Phần 2: 0000 11001

tổng độ dài vlc của rlc là: **1111 1111 1000 1010 0000 11001**

(8,-9) loại 4 phần 1:1111 1111 1011 1000 độ dài 20

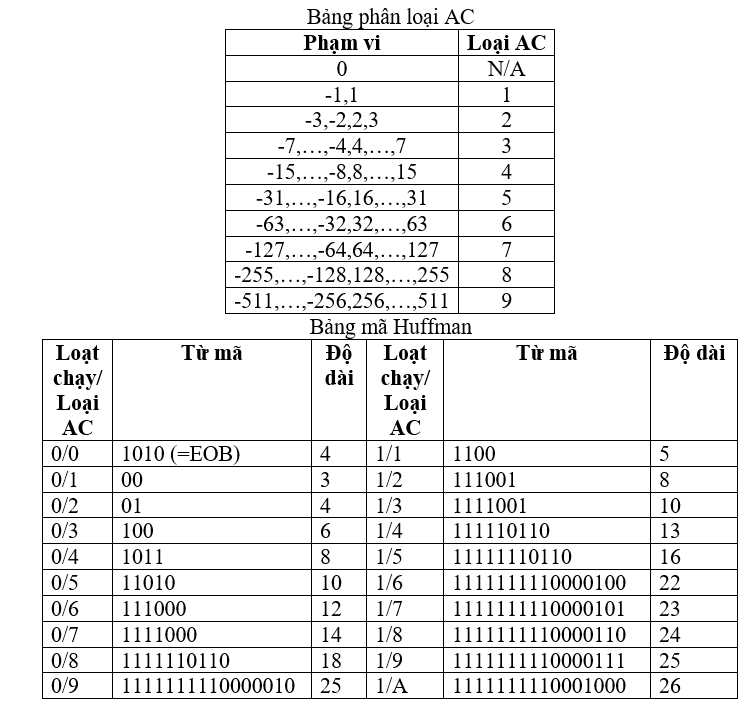
Phần 2:Biên độ 2^4-9-1=6: phần 2: 000000 110

Tổng độ dài vlc của rlc là: **1111 1111 1011 1000 000000 110**

**EOB: là 1010**

**Mã nhị phân là: 11110 1011000 1011 1100 100 101 0100 1111001 100** **1111 1111 1000 1010 0000 11001 1111 1111 1011 1000 000000 110 1010**

1. Thực hiện mã hóa độ dài thay đổi với từ mã độ dài chạy là (1,-25) với bảng phân loại giá trị AC và bảng mã Huffman được cho như sau:



**Giải:**

(1,-25)

2^4 <=25<2^5 => loại AC là 5

Từ bảng Huffman giá trị (1/5) có:

Mã phần 1: 1111 1110 110

Tổng độ dài 16=> phần 2 có 16-11=5bit

Biên độ : 2^5+(-25)-1=6

Mã phần 2 là:00110

Mã RLC là: 1111 1110 110 00110

1. Cho ma trận giá trị điểm ảnh như sau:

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 84 | 156 | 76 | 23 | 44 | 112 | 103 | 110 |
| 84 | 143 | 76 | 79 | 44 | 79 | 77 | 102 |
| 44 | 79 | 44 | 79 | 75 | 52 | 44 | 84 |
| 52 | 44 | 116 | 116 | 23 | 23 | 76 | 81 |
| 110 | 79 | 84 | 156 | 21 | 52 | 44 | 97 |
| 103 | 75 | 25 | 48 | 78 | 115 | 46 | 55 |
| 76 | 79 | 44 | 79 | 77 | 84 | 143 | 76 |
| 79 | 84 | 156 | 21 | 52 | 44 | 79 | 44 |

1. Hãy thực hiện nhúng tin m=0111 0101 0000 1101 1100 1101 theo thuật toán giấu và tìm kiếm tuần tự bắt đầu từ vị trí (hàng, cột)=(4,2).

**Giải**:

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 84 | 156 | 76 | 23 | 44 | 112 | 103 | 110 |
| 84 | 143 | 76 | 79 | 44 | 79 | 77 | 102 |
| 44 | 79 | 44 | 79 | 75 | 52 | 44 | 84 |
| 52 | 44 | **117** | **117** | **23** | **22** | **77** | **80** |
| **111** | **78** | **84** | **156** | **20** | **53** | **45** | **96** |
| **103** | **75** | **25** | **48** | **78** | **115** | **47** | **54** |
| **77** | 79 | 44 | 79 | 77 | 84 | 143 | 76 |
| 79 | 84 | 156 | 21 | 52 | 44 | 79 | 44 |

1. Trích xuất thông điệp từ ảnh có nhúng tin thu được từ câu a theo thuật toán giấu và tìm kiếm tuần tự.

**Giải**:

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 84 | 156 | 76 | 23 | 44 | 112 | 103 | 110 |
| 84 | 143 | 76 | 79 | 44 | 79 | 77 | 102 |
| 44 | 79 | 44 | 79 | 75 | 0 | 0 | 0 |
| 0 | 0 | **1** | **1** | **1** | **0** | **1** | **0** |
| **1** | **0** | **0** | **0** | **0** | **1** | **1** | **0** |
| **1** | **1** | **1** | **0** | **0** | **1** | **1** | **0** |
| **1** | 1 | 0 | 1 | 1 | 0 | 1 | 76 |
| 79 | 84 | 156 | 21 | 52 | 44 | 79 | 44 |

1. Biết ma trận đã cho đã nhúng thông điệp theo thuật toán giấu vào tìm kiếm tuần tự bắt đầu từ vị trí (hàng, cột)=(3,4), hãy tìm thông điệp ban đầu biết trước khi nhúng thông điệp đã được mã hóa bằng cách xor với khóa K=0001 1001 1100 111.

**Giải**:

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 84 | 156 | 76 | 23 | 44 | 112 | 103 | 110 |
| 84 | 143 | 76 | 79 | 44 | 79 | 77 | 102 |
| 44 | 79 | 44 | **1** | 1 | 0 | 0 | 0 |
| 0 | 0 | 0 | 0 | 1 | 1 | 0 | 1 |
| 0 | 1 | 0 | 0 | 1 | 0 | 0 | 1 |
| 1 | 1 | 1 | 0 | 0 | 1 | 0 | 1 |
| 76 | 79 | 44 | 79 | 77 | 84 | 143 | 76 |
| 79 | 84 | 156 | 21 | 52 | 44 | 79 | 44 |

Thông điệp mã hoá: 1100 0000 0110 101

Khoá K: 0001 1001 1100 111

Thông điệp: 1101 1001 1010 010

1. Biết khối ảnh dưới đây đã được nhúng tin theo thuật toán giấu và tìm kiếm tuần tự bắt đầu từ vị trí (hàng, cột)=(2,3). Thông điệp trước khi nhúng đã được mã hóa bằng cách xor với khóa K=0110 0111 0110 100. Hãy tìm thông điệp ban đầu.

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 42 | 75 | 50 | 72 | 42 | 106 | 134 | 80 |
| 125 | 125 | 22 | 50 | 42 | 75 | 75 | 134 |
| 104 | 150 | 11 | 42 | 50 | 72 | 42 | 104 |
| 125 | 125 | 22 | 50 | 22 | 50 | 42 | 42 |
| 80 | 75 | 104 | 150 | 11 | 42 | 55 | 22 |
| 75 | 42 | 125 | 125 | 22 | 50 | 42 | 42 |
| 104 | 107 | 51 | 76 | 42 | 75 | 75 | 134 |
| 104 | 150 | 50 | 22 | 42 | 106 | 134 | 80 |

**Giải:**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 42 | 75 | 50 | 72 | 42 | 106 | 134 | 80 |
| 125 | 125 | 0 | 0 | 0 | 1 | 1 | 0 |
| 0 | 0 | 1 | 0 | 0 | 0 | 0 | 0 |
| 1 | 1 | 0 | 50 | 22 | 50 | 42 | 42 |
| 80 | 75 | 104 | 150 | 11 | 42 | 55 | 22 |
| 75 | 42 | 125 | 125 | 22 | 50 | 42 | 42 |
| 104 | 107 | 51 | 76 | 42 | 75 | 75 | 134 |
| 104 | 150 | 50 | 22 | 42 | 106 | 134 | 80 |

Bản mã trích xuất: 0001 1000 1000 001

Khoá K : 0110 0111 0110 100

Thông điệp : 0111 1111 1 110 101

1. Cho ma trận giá trị điểm ảnh như sau:

|  |  |  |  |
| --- | --- | --- | --- |
| 51 | 76 | 42 | 75 |
| 42 | 75 | 50 | 72 |
| 125 | 125 | 22 | 50 |
| 104 | 150 | 11 | 42 |

Hãy nhúng tin m=1001011000 theo thuật toán giấu và tìm kiếm ngẫu nhiên theo yêu cầu xáo trộn dưới đây:

* Sắp xếp ma trận giá trị điểm ảnh thành véc tơ theo thứ tự từ trái qua phải từ trên xuống dưới.
* Sinh một chuỗi hỗn loạn gồm 16 phần tử theo công thức với và .
* Sắp xếp chuỗi hỗn loạn theo thứ tự tăng dần. Khóa hoán vị chuỗi sau khi sắp xếp chính là khóa xáo trộn các điểm ảnh của ảnh phủ.

**Giải**:

Sắp xếp ma trận:

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 51 | 76 | 42 | 75 | 42 | 75 | 50 | 72 | 125 | 125 | 22 | 50 | 104 | 150 | 11 | 42 |

Chương trình tạo khoá hỗn loạn

r= 3.9

x=0.8

b=[]

b.append(x)

print (x)

for a in range(1,16):

    x=r\*x\*(1-x)

    b.append(x)

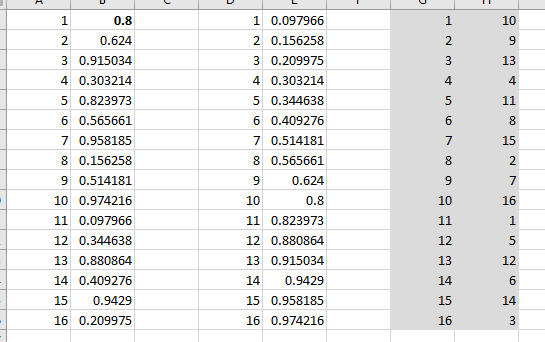
    print(x)

print("-----------------------------------------")

b.sort()

for i in b:

    print(i)



Từ kết quả trên sắp xếp lại ma trận theo đúng thứ tự:

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 51 | 76 | 42 | 75 | 42 | 75 | 50 | 72 | 125 | 125 | 22 | 50 | 104 | 150 | 11 | 42 |
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 22 | 72 | 42 | 75 | 50 | 150 | 125 | 75 | 76 | 51 | 42 | 104 | 42 | 11 | 50 | 125 |
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 |

Nhúng mẩu tin m=1001 0110 00 vào vị trí (1) trên thanh vừa đảo trên ta được

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 23 | 72 | 42 | 75 | 50 | 151 | 125 | 74 | 76 | 50 | 42 | 104 | 42 | 11 | 50 | 125 |
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 |

Xáo trộn cho về vị trí ban đầu

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 50 | 76 | 42 | 75 | 42 | 74 | 50 | 72 | 125 | 125 | 23 | 50 | 104 | 151 | 11 | 42 |
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 |

Đưa về ảnh ban đầu đã nhúng để gửi đi:

|  |  |  |  |
| --- | --- | --- | --- |
| 50 | 76 | 42 | 75 |
| 42 | 74 | 50 | 72 |
| 125 | 125 | 23 | 50 |
| 104 | 151 | 11 | 42 |

1. Cho ma trận giá trị điểm ảnh như sau:

|  |  |  |  |
| --- | --- | --- | --- |
| 22 | 75 | 42 | 75 |
| 75 | 42 | 125 | 125 |
| 80 | 75 | 104 | 150 |
| 75 | 42 | 125 | 125 |

Hãy nhúng tin m=1101101010 theo thuật toán giấu và tìm kiếm ngẫu nhiên theo yêu cầu dưới đây:

* Sắp xếp ma trận giá trị điểm ảnh thành véc tơ theo thứ tự từ trái qua phải từ dưới lên trên.
* Sinh một chuỗi hỗn loạn gồm 16 phần tử theo công thức với và
* Sắp xếp chuỗi hỗn loạn theo thứ tự giảm dần. Khóa hoán vị chuỗi sau khi sắp xếp chính là khóa xáo trộn các điểm ảnh của ảnh phủ.

**Giải**:

Sắp xếp lại ma trận:

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 75 | 42 | 125 | 125 | 80 | 75 | 104 | 150 | 75 | 42 | 125 | 125 | 22 | 75 | 42 | 75 |

Lấy chương trình sinh khoá bài trên thay 0.8 thành 0.4 và thêm hàm rev

r= 3.9

x=0.4

b=[]

b.append(x)

print (x)

for a in range(1,16):

    x=r\*x\*(1-x)

    b.append(x)

    print(x)

print("-----------------------------------------")

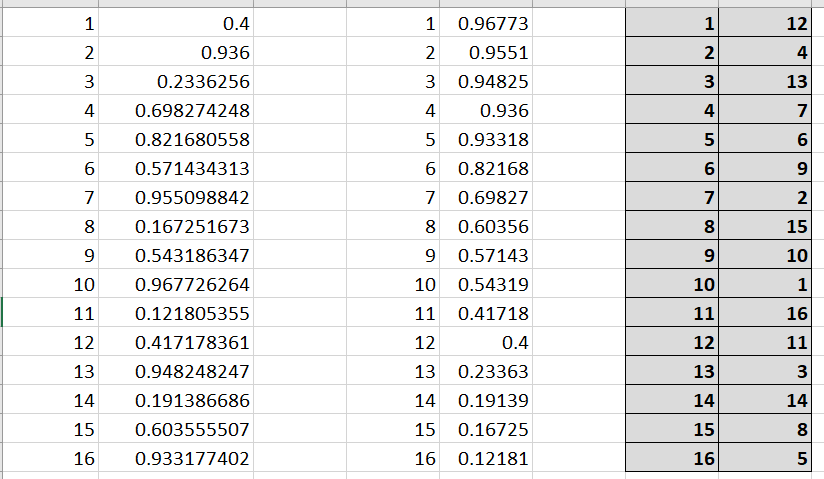
b.sort()

b.reverse()

for i in b:

    print(i)

chạy ctrinh trên thu được kq:



|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 75 | 42 | 125 | 125 | 80 | 75 | 104 | 150 | 75 | 42 | 125 | 125 | 22 | 75 | 42 | 75 |
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 |

Sắp xếp hỗn loạn

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 42 | 104 | 22 | 42 | 75 | 80 | 125 | 42 | 75 | 75 | 125 | 75 | 125 | 75 | 150 | 125 |
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 |

Thêm chuỗi m=1101 1010 10 vào :

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 43 | 105 | 22 | 43 | 75 | 80 | 125 | 42 | 75 | 74 | 125 | 75 | 22 | 75 | 150 | 125 |
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 |

Quay về vector ban đầu:

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 75 | 43 | 22 | 125 | 80 | 75 | 105 | 150 | 74 | 43 | 125 | 125 | 22 | 75 | 42 | 75 |
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 |

Quay về ảnh gửi đi:

|  |  |  |  |
| --- | --- | --- | --- |
| 22 | 75 | 42 | 75 |
| 74 | 43 | 125 | 125 |
| 80 | 75 | 105 | 150 |
| 75 | 43 | 22 | 125 |

1. Cho ma trận điểm ảnh của ảnh phủ C:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 47 | 59 | 38 | 41 | 38 | 53 |
| 44 | 51 | 49 | 34 | 43 | 49 |
| 57 | 46 | 38 | 37 | 43 | 57 |
| 51 | 68 | 53 | 49 | 42 | 50 |
| 48 | 51 | 43 | 47 | 47 | 55 |
| 32 | 47 | 48 | 42 | 46 | 42 |

Khóa k gồm các tham số (a, p) = (17 ,37). Xáo trộn các điểm ảnh của C theo công thức: yi = ai mod p. Với yi là vị trí xáo trộn của điểm ảnh thứ i trong C

Áp dụng thuật toán giấu và tìm kiếm ngẫu nhiên, em hãy nhúng thông điệp m = 0100111011 và trích xuất thông tin từ ma trận ảnh stego thu được.

Giải:

Ta có công thức y­­i=17imod37

Với i = 1 thì y=17

i=2 thì y=30

i=3 thì y=29

…..

Thực hiện đổi hết ta được mảng mới

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 43 | 55 | 47 | 49 | 51 | 43 |
| 38 | 48 | 53 | 47 | 47 | 51 |
| 46 | 38 | 46 | 37 | 57 | 42 |
| 68 | 44 | 51 | 48 | 57 | 34 |
| 49 | 41 | 32 | 49 | 38 | 43 |
| 59 | 42 | 42 | 53 | 50 | 47 |

Nhúng thông điệp m= 0100111011 vào mảng sau khi đã hoán đổi vị trí

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 42 | 55 | 46 | 48 | 51 | 43 |
| 39 | 48 | 53 | 47 | 47 | 51 |
| 46 | 38 | 46 | 37 | 57 | 42 |
| 68 | 44 | 51 | 48 | 57 | 34 |
| 49 | 41 | 32 | 49 | 38 | 43 |
| 59 | 42 | 42 | 53 | 50 | 47 |

Khôi phục về ảnh ban đầu sau khi nhúng

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 47 | 59 | 38 | 41 | 38 | 53 |
| 44 | 51 | 49 | 34 | 43 | 48 |
| 57 | 46 | 39 | 37 | 42 | 57 |
| 51 | 68 | 53 | 49 | 42 | 50 |
| 48 | 51 | 43 | 47 | 46 | 55 |
| 32 | 47 | 48 | 42 | 46 | 42 |

Trích xuất ngược lại nhúng .

1. Cho ma trận giá trị điểm ảnh như sau:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 107 | 51 | 76 | 42 | 75 | 75 |
| 75 | 42 | 75 | 50 | 72 | 42 |
| 42 | 125 | 125 | 22 | 50 | 42 |
| 75 | 104 | 150 | 11 | 42 | 55 |
| 42 | 125 | 125 | 22 | 50 | 42 |
| 107 | 51 | 76 | 42 | 75 | 75 |

Hãy nhúng tin m=0110001001001010 theo thuật toán giấu và tìm kiếm ngẫu nhiên theo yêu cầu dưới đây:

* Sinh khóa theo công thức với a và .
* Xáo trộn khối điểm ảnh theo khóa vừa nhận được với ứng với vị trí điểm ảnh hiện tại và ứng với vị trí của điểm ảnh sau xáo trộn.

1. Áp dụng thuật toán giấu tin trong khối bit Wu-Lee để thực hiện nhúng và trích xuất chuỗi bit B=0110 vào ảnh F sử dụng khóa K với các giả thiết như sau:

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| F =   |  |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | --- | | 0 | 1 | 0 | 1 | 1 | 1 | 1 | 0 | | 0 | 1 | 1 | 1 | 0 | 1 | 0 | 0 | | 0 | 1 | 1 | 0 | 1 | 1 | 0 | 1 | | 1 | 0 | 1 | 0 | 0 | 1 | 0 | 1 | | 1 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | | 1 | 0 | 1 | 0 | 0 | 1 | 0 | 1 | | 0 | 1 | 0 | 0 | 1 | 0 | 1 | 0 | | 1 | 0 | 1 | 1 | 0 | 0 | 1 | 0 | | K =   |  |  |  |  | | --- | --- | --- | --- | | 1 | 0 | 0 | 1 | | 0 | 0 | 1 | 0 | | 0 | 1 | 1 | 1 | | 1 | 1 | 1 | 0 | |

1. Áp dụng thuật toán giấu tin trong khối bit Wu-Lee để thực hiện nhúng và trích xuất chuỗi bit B=1010 vào ảnh F sử dụng khóa K với các giả thiết như sau:

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| F =   |  |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | --- | | 1 | 0 | 0 | 0 | 1 | 0 | 1 | 0 | | 0 | 1 | 1 | 1 | 1 | 1 | 1 | 0 | | 0 | 0 | 1 | 1 | 0 | 1 | 1 | 0 | | 0 | 1 | 0 | 0 | 1 | 0 | 0 | 1 | | K =   |  |  |  |  | | --- | --- | --- | --- | | 1 | 1 | 0 | 1 | | 0 | 1 | 1 | 1 | |

1. Áp dụng thuật toán giấu tin trong khối bit Wu-Lee để thực hiện nhúng và trích xuất chuỗi bit B=0011 vào ảnh F sử dụng khóa K với các giả thiết như sau:

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| F =   |  |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | --- | | 1 | 0 | 0 | 0 | 1 | 0 | 1 | 0 | | 0 | 1 | 1 | 1 | 1 | 1 | 1 | 0 | | 0 | 0 | 1 | 1 | 0 | 1 | 1 | 0 | | 0 | 1 | 0 | 0 | 1 | 0 | 0 | 1 | | K =   |  |  | | --- | --- | | 1 | 1 | | 0 | 1 | | 1 | 1 | | 0 | 0 | |

1. Áp dụng thuật toán giấu tin trong khối bit Wu-Lee để thực hiện nhúng và trích xuất chuỗi bit B=1000 vào ảnh F sử dụng khóa K với các giả thiết như sau:

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| F =   |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | | 1 | 0 | 0 | 0 | 1 | 0 | | 0 | 1 | 1 | 1 | 1 | 1 | | 0 | 0 | 1 | 1 | 0 | 1 | | 0 | 1 | 0 | 0 | 1 | 0 | | 0 | 0 | 0 | 1 | 0 | 1 | | 1 | 1 | 1 | 1 | 0 | 0 | | 0 | 1 | 1 | 0 | 1 | 1 | | 1 | 0 | 0 | 1 | 0 | 1 | | K =   |  |  |  | | --- | --- | --- | | 1 | 1 | 0 | | 0 | 1 | 0 | | 1 | 1 | 1 | | 0 | 0 | 1 | |

1. Áp dụng thuật toán giấu tin trong khối bit Wu – Lee thực hiện nhúng và trích xuất tin B = 010 vào ảnh F sử dụng khóa K, với các giả thiết cho ở dưới.

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Ảnh F   |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | | 1 | 1 | 0 | 1 | 0 | 1 | | 1 | 0 | 1 | 1 | 1 | 1 | | 0 | 1 | 1 | 0 | 1 | 0 | | 0 | 1 | 0 | 1 | 1 | 1 | | 1 | 1 | 1 | 0 | 0 | 0 | | 0 | 1 | 1 | 1 | 0 | 0 | | Khóa K   |  |  |  | | --- | --- | --- | | 0 | 1 | 0 | | 1 | 1 | 1 | | 0 | 1 | 1 | |

1. Cho ma trận điểm ảnh 8x8 như sau

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Q1 | 1 | 0 | 1 | 0 | 0 | 0 | 1 | 1 | Q5 |
|  | 0 | 1 | 1 | 1 | 0 | 0 | 1 | 1 |  |
| Q2 | 1 | 0 | 1 | 1 | 0 | 0 | 0 | 1 | Q6 |
|  | 0 | 1 | 1 | 0 | 1 | 1 | 0 | 1 |  |
| Q3 | 1 | 0 | 1 | 1 | 0 | 1 | 1 | 0 | Q7 |
|  | 1 | 1 | 0 | 0 | 1 | 0 | 1 | 0 |  |
| Q4 | 1 | 0 | 1 | 1 | 0 | 1 | 1 | 1 | Q8 |
|  | 0 | 0 | 1 | 1 | 0 | 1 | 1 | 1 |  |

Khóa K

|  |  |  |  |
| --- | --- | --- | --- |
| 0 | 1 | 0 | 1 |
| 1 | 0 | 1 | 1 |

1. Sử dụng thuật toán Wu-Lee ẩn tin m, với m = (SBD mod 23) + 13 và được biểu diễn dưới dạng 8 bít, vào các khối Q trong ma trận trên.
2. Khối trên được ẩn mã độ dài tối đa 8 bít, với phân chia các khối con như trên sử dụng khóa

|  |  |  |  |
| --- | --- | --- | --- |
| 1 | 0 | 1 | 1 |
| 1 | 1 | 0 | 0 |

Hãy trích xuất mã được ẩn trong ma trận trên.

1. Cho ma trận hệ số DCT của một khối ảnh như sau:

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| -415 | -30 | -61 | 0 | 0 | 0 | 1 | 0 |
| 4 | 0 | 1 | 5 | 21 | 4 | 0 | 0 |
| 15 | 1 | 0 | 0 | 7 | 0 | -24 | 0 |
| 12 | 0 | 1 | 13 | 1 | 1 | 1 | 1 |
| 1 | 1 | 0 | 0 | 0 | 17 | 0 | 0 |
| 23 | 0 | -19 | 1 | 0 | 1 | 0 | 1 |
| 0 | 0 | 0 | 0 | 1 | 18 | 1 | 0 |
| 1 | 1 | 0 | 0 | 1 | 0 | 1 | 1 |

Ma trận trên đã được nhúng thông điệp theo thuật toán Jsteg bắt đầu từ vị trí (hàng, cột)=(1,5). Tìm chuỗi thông điệp ban đầu biết trước khi nhúng thông điệp đã được xor với khóa K=001100111001.

**Giải**: Ma trận sau khi trích xuất

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| -415 | -30 | -61 | 0 | 0 | 0 | 1 | 0 |
| 0 | 0 | 1 | 1 | 1 | 0 | 0 | 0 |
| 1 | 1 | 0 | 0 | 1 | 0 | 1 | 0 |
| 0 | 0 | 1 | 1 | 1 | 1 | 1 | 1 |
| 1 | 1 | 0 | 0 | 0 | 1 | 0 | 0 |
| 1 | 0 | 1 | 1 | 0 | 1 | 0 | 1 |
| 0 | 0 | 0 | 0 | 1 | 0 | 1 | 0 |
| 1 | 1 | 0 | 0 | 1 | 0 | 1 | 1 |

Vì nhúng từ đoạn (1,5) nên sẽ trích xuất từ đoạn (1,5)

Tin nhắn trích xuất: 0110 1110 1111

Khoá K : 0011 0011 1001

Tin nhắn ban đầu: : 0101 1101 0110

1. Cho ma trận hệ số DCT của một khối ảnh như sau:

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| -415 | -30 | -61 | 0 | 0 | 0 | 1 | 0 |
| 4 | 0 | 1 | 5 | 21 | 4 | 0 | 0 |
| 15 | 1 | 0 | 0 | 0 | 0 | 0 | 0 |
| 12 | 0 | 1 | 13 | 1 | 1 | 1 | 1 |
| 1 | 1 | 0 | 0 | 0 | 17 | 0 | 0 |
| 23 | 0 | -19 | 1 | 0 | 1 | 0 | 1 |
| 0 | 0 | 0 | 0 | 1 | 18 | 1 | 0 |
| 1 | 1 | 0 | 0 | 1 | 0 | 1 | 1 |

1. Dựa trên thuật toán ẩn mã Outguess hãy tạo chuỗi giả ngẫu bằng cách sắp xếp zig-zag, sau đó dịch vòng phải k=2 vị trí.

Giải: xếp zig-zag:

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| -415 | -30 | 4 | 15 | 0 | -61 | 0 | 1 |
| 1 | 12 | 1 | 0 | 0 | 5 | 0 | 0 |
| 21 | 0 | 1 | 1 | 23 | 0 | 0 | 0 |
| 13 | 0 | 4 | 1 | 0 | 0 | 0 | 1 |
| 0 | -19 | 0 | 1 | 1 | 0 | 1 | 0 |
| 1 | 0 | 0 | 0 | 1 | 17 | 0 | 0 |
| 0 | 0 | 1 | 1 | 0 | 1 | 0 | 0 |

Dịch vòng phải k=2:

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 4 | 15 | 0 | -61 | 0 | 1 | -415 | -30 |
| 1 | 0 | 0 | 5 | 0 | 0 | 1 | 12 |
| 1 | 1 | 23 | 0 | 0 | 0 | 21 | 0 |
| 4 | 1 | 0 | 0 | 0 | 1 | 13 | 0 |
| 0 | 1 | 1 | 0 | 1 | 0 | 0 | -19 |
| 0 | 0 | 1 | 17 | 0 | 0 | 1 | 0 |
| 1 | 1 | 0 | 1 | 0 | 0 | 0 | 0 |
| 0 | 1 | 1 | 0 | 1 | 1 | 18 | 1 |

1. Thực hiện nhúng thông điệp m=1001000111.

Nhúng thông điệp m= 1001 0001 11

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 4 | 15 | 0 | -60 | 0 | 1 | -414 | -31 |
| 1 | 0 | 0 | 4 | 0 | 0 | 1 | 12 |
| 1 | 1 | 22 | 0 | 0 | 0 | 20 | 0 |
| 4 | 1 | 0 | 0 | 0 | 1 | 13 | 0 |
| 0 | 1 | 1 | 0 | 1 | 0 | 0 | -19 |
| 0 | 0 | 1 | 17 | 0 | 0 | 1 | 0 |
| 1 | 1 | 0 | 1 | 0 | 0 | 0 | 0 |
| 0 | 1 | 1 | 0 | 1 | 1 | 18 | 1 |

Quay về ảnh ban đầu:

Quay vòng trái k=2 để vể ảnh zig-zag

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| -414 | -31 | 4 | 15 | 0 | -60 | 0 | 1 |
| 1 | 12 | 1 | 0 | 0 | 4 | 0 | 0 |
| 21 | 0 | 1 | 1 | 22 | 0 | 0 | 0 |
| 13 | 0 | 4 | 1 | 0 | 0 | 0 | 1 |
| 0 | -19 | 0 | 1 | 1 | 0 | 1 | 0 |
| 1 | 0 | 0 | 0 | 1 | 17 | 0 | 0 |
| 0 | 0 | 1 | 1 | 0 | 1 | 0 | 0 |
| 18 | 1 | 0 | 1 | 1 | 0 | 1 | 1 |

Zig-zag ngược để về ảnh ban đầu:

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| -414 | -31 | -60 | 0 | 0 | 0 | 1 | 0 |
| 4 | 0 | 1 | 5 | 20 | 4 | 0 | 0 |
| 15 | 1 | 0 | 0 | 0 | 0 | 0 | 0 |
| 12 | 0 | 1 | 13 | 1 | 1 | 1 | 1 |
| 1 | 1 | 0 | 0 | 0 | 17 | 0 | 0 |
| 22 | 0 | -19 | 1 | 0 | 1 | 0 | 1 |
| 0 | 0 | 0 | 0 | 1 | 18 | 1 | 0 |
| 1 | 1 | 0 | 0 | 1 | 0 | 1 | 1 |

1. Biết ma trận hệ số trên đã được nhúng thông điệp bằng thuật toán Jsteg theo chiều từ trên xuống dưới từ trái qua phải và thông điệp trước khi nhúng đã được xor với khóa K=1110100101. Hãy tìm thông điệp ban đầu.

Mảng sau khi trích xuất theo độ dài khoá K

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| -414 | 1 | 0 | 0 | 0 | 0 | 1 | 0 |
| 0 | 0 | 1 | 1 | 0 | 0 | 0 | 0 |
| 1 | 1 | 0 | 0 | 0 | 0 | 0 | 0 |
| 0 | 0 | 1 | 1 | 1 | 1 | 1 | 1 |
| 1 | 1 | 0 | 0 | 0 | 1 | 0 | 0 |
| 22 | 0 | -19 | 1 | 0 | 1 | 0 | 1 |
| 0 | 0 | 0 | 0 | 1 | 18 | 1 | 0 |
| 1 | 1 | 0 | 0 | 1 | 0 | 1 | 1 |

Thông điệp trích xuất: 1001 0010 11

Khoá K : 1110 1001 01

Thông điệp ban đầu : 0111 1011 10

1. Cho ma trận các hệ số DCT 8 x 8 như sau:

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 1480 | 51 | -71 | 0 | 0 | 0 | 1 | 0 |
| 10 | 0 | 23 | -22 | 10 | 7 | 0 | 0 |
| 1 | 1 | 0 | 0 | 0 | 0 | 0 | 0 |
| -13 | 0 | 1 | 13 | 1 | 1 | 1 | 1 |
| 1 | 1 | 0 | 0 | 0 | 1 | 0 | 0 |
| -34 | 0 | -29 | 1 | 0 | 1 | 0 | 1 |
| 0 | 0 | 0 | 0 | 1 | -6 | 1 | 0 |
| 1 | 1 | 0 | 0 | 1 | 0 | 1 | 1 |

* 1. Dựa trên thuật toán Outguess, yêu cầu:
     + Tạo chuỗi giả ngẫu nhiên DCT bằng cách trích rút các hệ số DCT trên theo sắp xếp zig – zag, sau đó dịch vòng theo chiều tử trên xuống k = 3 hàng
     + Thực hiện ẩn tin m = 01101011 trong khối ma trận trên
     + Thực hiện trích xuất tin mật thu được sau khi ẩn tin

Xắp xếp zig-zag:

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 1480 | 51 | 10 | 1 | 0 | -71 | 0 | 23 |
| 1 | -13 | 1 | 0 | 0 | -22 | 0 | 0 |
| 10 | 0 | 1 | 1 | -34 | 0 | 0 | 0 |
| 13 | 0 | 7 | 1 | 0 | 0 | 0 | 1 |
| 0 | -29 | 0 | 1 | 1 | 0 | 1 | 0 |
| 1 | 0 | 0 | 0 | 1 | 1 | 0 | 0 |
| 0 | 0 | 1 | 1 | 0 | 1 | 0 | 0 |
| -6 | 1 | 0 | 1 | 1 | 0 | 1 | 1 |

Dịch vòng xuống k=3 hàng:

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 1 | 0 | 0 | 0 | 1 | 1 | 0 | 0 |
| 0 | 0 | 1 | 1 | 0 | 1 | 0 | 0 |
| -6 | 1 | 0 | 1 | 1 | 0 | 1 | 1 |
| 1480 | 51 | 10 | 1 | 0 | -71 | 0 | 23 |
| 1 | -13 | 1 | 0 | 0 | -22 | 0 | 0 |
| 10 | 0 | 1 | 1 | -34 | 0 | 0 | 0 |
| 13 | 0 | 7 | 1 | 0 | 0 | 0 | 1 |
| 0 | -29 | 0 | 1 | 1 | 0 | 1 | 0 |

Thực hiện ẩn tin m=0110 1011

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 1 | 0 | 0 | 0 | 1 | 1 | 0 | 0 |
| 0 | 0 | 1 | 1 | 0 | 1 | 0 | 0 |
| -6 | 1 | 0 | 1 | 1 | 0 | 1 | 1 |
| 1481 | 51 | 10 | 1 | 0 | -70 | 0 | 23 |
| 1 | -12 | 1 | 0 | 0 | -23 | 0 | 0 |
| 11 | 0 | 1 | 1 | -34 | 0 | 0 | 0 |
| 13 | 0 | 7 | 1 | 0 | 0 | 0 | 1 |
| 0 | -29 | 0 | 1 | 1 | 0 | 1 | 0 |

* 1. Ma trận các hệ số DCT trên đã ẩn mã có độ dài 8 bít dựa trên thuật toán Jsteg và sử dụng trích rút các hệ số lần lượt theo chiều ngang, từ trái sang phải và từ trên xuống dưới. Hãy trích xuất tin nhúng trong ma trận nêu trên.

1. Cho ma trận hệ số DCT của một khối ảnh như sau:

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| -415 | -31 | -64 | 0 | 0 | 16 | 1 | 0 |
| 5 | 0 | 1 | 5 | 21 | 4 | 0 | 0 |
| 15 | 1 | 0 | 0 | 0 | 0 | 0 | 0 |
| 12 | 0 | 1 | 13 | 1 | 1 | 1 | 1 |
| 1 | 7 | 0 | 0 | 0 | 17 | 0 | 0 |
| 23 | 0 | -19 | 1 | 0 | 1 | 0 | 1 |
| 0 | 0 | 0 | 0 | 1 | 18 | 1 | 0 |
| 1 | 1 | 0 | 0 | 1 | 0 | 1 | 1 |

Hãy trích xuất thông điệp trong khối DCT trên biết thông điệp đã nhúng theo thuật toán Outguess với phương pháp xáo trộn là sắp xếp zigzag đã học.