**CMSE-492 MT Exam 16.04.2019 (110 min, 20 points)**

St. **Name, Surname**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_St.Id#\_\_\_\_\_\_\_\_\_\_\_\_\_

**Instructor Alexander Chefranov**

Totally 4 questions, 14 pages

**Task 1. (5 points)** Embed secret bits from S=’1001 0111 0110 0111’ into the cover image, CI=(10,216) by Wang’s Modulo operator method using T=160, ml=16, mu=32. Check correctness of embedding by extraction. Show details of your calculations, give necessary explanations.

**Hint: Wang’s method Embedding and Extraction**

****

****

****

****

****

****

Embedding into P1=10<T=160, hence, Case 1, EC=log2(16)=4 bits, Res=P1 mod ml =10 mod 16 = 10. Dec= 10012=9. D=|Res-Dec| = |10-9|=1. ml/2=8<=P1<T-ml/2=160-16/2=152. D<=ml/2=16/2=8, AV=D=1. Res=10>Dec=9 => Ps(1)=Pc(1)-AV = 10-1=9.

Extraction: Ps(1)=9<T=160, hence, Case 1, EC=log2(16)=4, Res=Ps(1) mod ml = 9 mod 16 = 9= 10012 that coincides with the embedded binary data 10012.

Embedding into P2=216>T=160, hence, Case 2, EC=log2(32)=5 bits, Res=P2 mod mu =216 mod 16 = 24. Dec= 011102=14. D=|Res-Dec| = |24-14|=10. T+mu/2=176<=P2<255-mu//2+1=255-32/2+1=240. D=10<=mu/2=32/2=16, AV=D=10. Res=24>Dec=14 => Ps(2)=Pc(2)-AV = 216-10=206.

Extraction: Ps(2)=206>T=160, hence, EC=log2(32)=5, Res=Ps(2) mod mu = 206 mod 16 = 14= 0111102 that coincides with the embedded binary data 011102.

**Task 2. (5 points)** Embed secret bits from S=’1001 0111 0110 0111’ into the cover image, CI=(10,216) by Wu and Tsai Pixel-value differencing method using ranges R1=[0,7], R2=[8,15], R3=[16,31], R4=[32,63], R5=[64,127], R6=[128,255]. Before embedding, check that the pixel pair is to be used/not used for embedding.

Extract the data embedded. Before extraction, check the pixel pair for the abandonment condition; check that the condition returns exactly the same result as it was when checking for embedding this pair. Show details of your calculations, give necessary explanations.

**Hint:**









Embedding: d=p2-p1=216-10=206 belongs to R6, l6=128, u6=255, n=log2(u6-l6+1)=log2(128)=7, b=10010112=75, d’=l6+b=128+75=203. Check falling-off boundary condition. F((p1,p2),u6-d)=f((10,216),255-206)=f((10,216),49)=|floorm=floor(49/2)=24, ceilm=ceil(49/2)=25, d is even| = (p1- floorm,p2+ ceilm)=(10-24, 216+25)=(-14, 241) . Because we get negative 1st pixel, falling-off boundary happens, and we don’t embed into the pair.

Extraction: As far as the pixels in the embedding are not changed, in the extraction the falling-off boundary condition also holds, and no extraction is done from that pair.

**Task 3. (5 points)** Embed secret bits from S=’1001 0111 0110 0111’ into the cover image, CI=(10, 216) by Khodaei et al. Hybrid method. Extract the data embedded from the stego pixels. Show details of your calculations, give necessary explanations.

**Hints:**

****

****

****

****

Embedding: since p2=216>=192, Case 2 is applied. d=|p1-p2|=196, it belongs to R4=[128, 255], and k=7 bits shall be LSB embedded into each pixel of the pair. Bs1=10010112=75, bs2=10110012=89. Ps1=p1- p1 mod 128 +bs1 = 75, ps2=p2 – p2 mod 128 + bs2 = 216 – 216 mod128 + 89 = 216-88+89=217. D’=|217-75|=142 is from R4, hence readjustment is not applied.

Extraction: (ps1, ps2)=(75, 217), ps2>192, hence, Case 2 is applied. d’=|217-75|=142 is from R4=[128, 255], hence k=7 bits are LSB extracted from each pixel. Bs1= ps1 mod 128 = 75 mod 128 = 75 = 10010112 that is the same as embedded into p1, bs2 = ps2 mod 128 = 217 mod 128 = 89 = 10110012 that is the same as embedded into p2.

**Task 4.**  **(5 points)** Consider the grayscale image, I, below having 1 row and 8 columns:

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | Col1 | Col2 | Col3 | Col4 | Col5 | Col6 | Col7 | Col8 |
| Row1 | 255 | 254 | 3 | 52 | 251 | 250 | 0 | 1 |

**U**se EMD method to embed secret bits ’1001 0111 0110 0111’ using L=16, n=4. Define number K of (2n+1)-ary digits in a block. Show details of your calculations. Check correctness of embedding by extraction. Give necessary explanations.

**Hints:**









We shall have $2^{L}=2^{16}=65536\leq \left(2n+1\right)^{K}=\left(2∙4+1\right)^{K}=9^{K}$

$9^{5}=59049<65536$, hence, K=6.

Convert 16 bits into hexadecimal and to decimal: 1001 0111 0110 0111=976716=9\*163+7\*162+6\*16+7=9\*4096+7\*256+6\*16+7= 36864+1792+96+7=38759

Convert the decimal to 6-digit 9-ary notational system

38759 div 9=4306 38759 mod 9=5

4306 div 9=478 4306 mod 9=4

478 div 9=53 478 mod 9=1

53 div 9=5 53 mod 9=8. Hence, 6-digit 9-ary secret stream is 0581459=5\*94+8\*93+1\*92+4\*9+5=5\*6561+8\*729+81+36+5=32805+5832+122=38759 that is the same as in decimal

Now, embed the 1st digit, d=0, into the 1st pixel group=(255, 254, 3, 52). Calculate extraction function:

f=F(255,254,3,52)=255+254\*2+3\*3+52\*4 mod 9= 3+2\*2+9+7\*4 mod 9=7+1 mod 9 = 8

s=d-f mod 9=0-8=-8 mod 9 =1. Hence, we need increasing p1 by 1 getting 255+1=256 that is out of boundary. Hence, we decrease p1=p1-1=254 and retry embedding d intp the group: f=F(254,254,3,52)=254+254\*2+3\*3+52\*4 mod 9= 2+2\*2+9+7\*4 mod 9=6+1 mod 9 = 7, s=d-f mod 9 = 0-7=-7 mod 9 = 2. Hence, we embed d by increasing p2=p2+1=254+1=255, and the stego pixel group is (254, 255, 3,52).

Extraction: Calculate extraction function on the stego group

d=f=F(254,255,3,52)=254+255\*2+3\*3+52\*4 mod 9= 2+3\*2+9+7\*4 mod 9=8+1 mod 9 =0 that is equal to the 1st digit embedded.

Embed the 2nd digit, d=5, into the 2nd group (251,250,0,1).

f=F(251.250,0,1)=251+250\*2+0\*3+1\*4=8+7\*2+0+4 mod 9 = 8+14+4 mod 9 = 8

s=d-f mod 9 = 5-8 mod 9 = -3 mod 9 = 6>4. Hence, we decrease by p(9-6)=p3: p3’=p3-1=-1, that is out of boundaries. Hence, we increase, p3 by 1: p3=p3+1=1+1=2, and repeat embedding: f=F(251.250,1,1)=251+250\*2+1\*3+1\*4=8+7\*2+3+4 mod 9 = 8+14+3+4 mod 9 = 2, s=d-f mod 9 = 5-2 mod 9 = 3<4, hence, we embed by increasing p3: p3=p3+1=1+1=2 getting stego group (251, 250, 2,1) Extract now from the 2nd group:

s=f=F(251.250,2,1)=251+250\*2+2\*3+1\*4=8+7\*2+6+4 mod 9 = 8+14+6+4 mod 9 = 5 that is equal to the digit d=5 embedded.