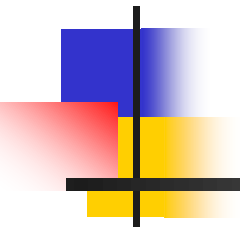
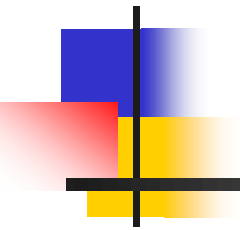


变换域隐秘技术

变换域隐秘技术

- DCT域的信息隐秘
- 小波域的信息隐秘



DCT域的信息隐秘

第一部分

秘密信息的隐写

DCT域的信息隐秘

用下面的公式实现一个矩阵的二维DCT变换：

$$B_{pq} = a_p a_q \sum_{m=0}^{M-1} \sum_{n=0}^{N-1} A_{mn} \cos \frac{\pi(2m+1)p}{2M} \cos \frac{\pi(2n+1)q}{2N}$$

$$0 \le p \le M-1 \qquad 0 \le q \le N-1$$

$$a_p = \begin{cases} \frac{1}{\sqrt{M}}, p=0 \\ \sqrt{\frac{2}{M}}, 1 \le p \le M-1 \end{cases} \qquad a_q = \begin{cases} \frac{1}{\sqrt{N}}, q=0 \\ \sqrt{\frac{2}{N}}, 1 \le q \le N-1 \end{cases}$$

DCT域的信息隐秘

逆DCT变换定义如下：

$$A_{mn}=\sum_{p=0}^{M-1}\sum_{q=0}^{N-1}a_p a_q B_{pq}\cos\frac{\pi(2m+1)p}{2M}\cos\frac{\pi(2n+1)q}{2N}$$

$$0\le m\le M-1 \qquad 0\le n\le N-1$$

DCT域的信息隐秘

信息隐秘的总体思想就是：通过调整图像块中两个DCT系数的相对大小来对秘密信息进行编码。我们用(u1,v1),(u2,v2)来表示这两个系数的索引，算法描述如下：

对于第i bit秘密信息

if (要隐藏信息‘1’)

make $(u1,v1)_i > (u2,v2)_i$;

else

make $(u1,v1)_i < (u2,v2)_i$;

DCT域的信息隐秘

我们引用JPEG压缩方案中的亮度量化表：

(u,v)	1	2	3	4	5	6	7	8
1	16	11	10	16	24	40	51	61
2	12	12	14	19	26	58	60	55
3	14	13	16	24	40	57	69	56
4	14	17	22	29	51	87	80	62
5	18	22	37	56	68	109	103	77
6	24	35	55	64	81	104	113	92
7	49	64	78	87	103	121	120	101
8	72	92	95	98	112	100	103	99

DCT域的信息隐秘

为了让一幅图像中隐藏尽可能多的秘密信息，我们需要把图像分块，每一块中编码一个秘密信息，一般选择8×8的图像块。基于量化系数一致和兼顾机密信息隐藏的不可见性与鲁棒性等因素，选择量化表中(5,2)和(4,3)这一对系数或者(2,3)和(4,1)这一对系数来完成信息的隐秘。

DCT域的信息隐秘

同时，我们引入一个控制量α对系数差值进行放大。在编码的过程中，无论是$B_i(u1,v1)>B_i(u2,v2)$或是$B_i(u1,v1)<B_i(u2,v2)$我们都要使得$|B_i(u1,v1)-B_i(u2,v2)|>\alpha$，这样，即使在变换过程中系数的值有轻微的改变，也不会影响编码的正确性 。

DCT域的信息隐秘

选择lenna图像作为载体，隐藏的信息是一以.txt文件保存的字符串。我们取密钥为1982，控制阈值α取为1。

DCT域的信息隐秘

下面分别是原始图像和嵌入信息后的图像：

DCT域的信息隐秘

图像被分成8×8的块，k1，k2分别标识各块的首行地址和列地址，来依次选择编码的块。

```
k1 =
  Columns 1 through 14

     1     1     1     1     1     1     1     1     1     2     2     2     2     2

  Columns 15 through 28

     2     2     2     2     2     3     3     3     3     3     3     3     3     3

  Columns 29 through 42

     3     4     4     4     4     4     4     4     4     4     4     4     5     5

  Columns 43 through 56
...
```

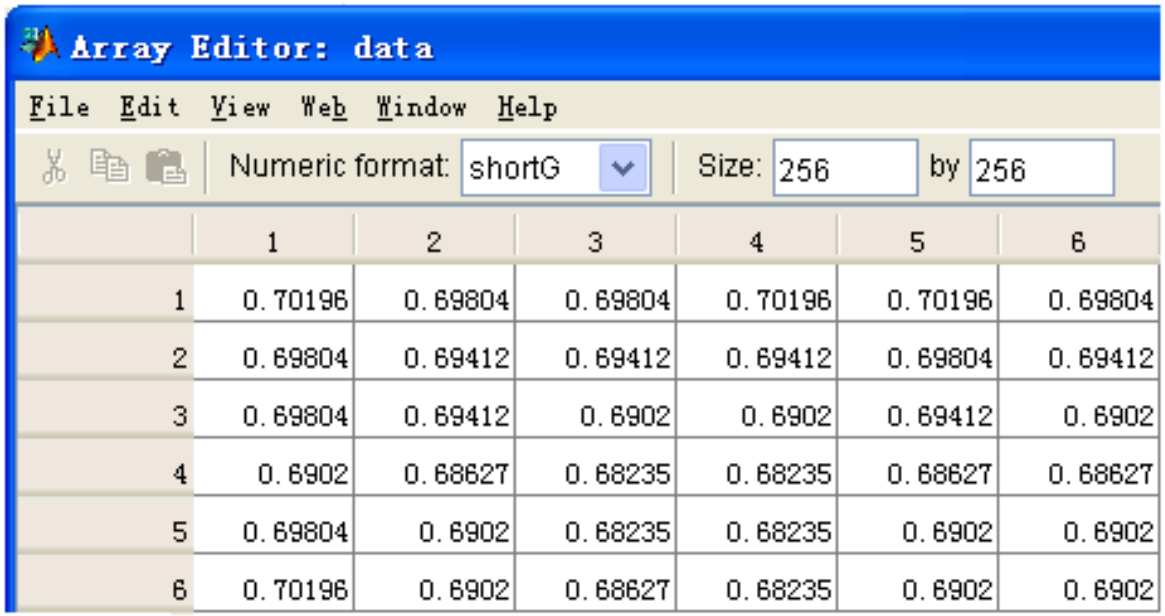
DCT域的信息隐秘

```
k2 =
  Columns 1 through 14

     1     5     7     9    13    17    21    25    29     1     5     7     9    13

  Columns 15 through 28

    17    21    23    27    31     1     3     7     9    13    17    19    23    25

  Columns 29 through 42

    29     1     5     7    11    13    15    19    23    25    29    31     3     7

  Columns 43 through 56
...
```

DCT域的信息隐秘

下面是一些中间结果：

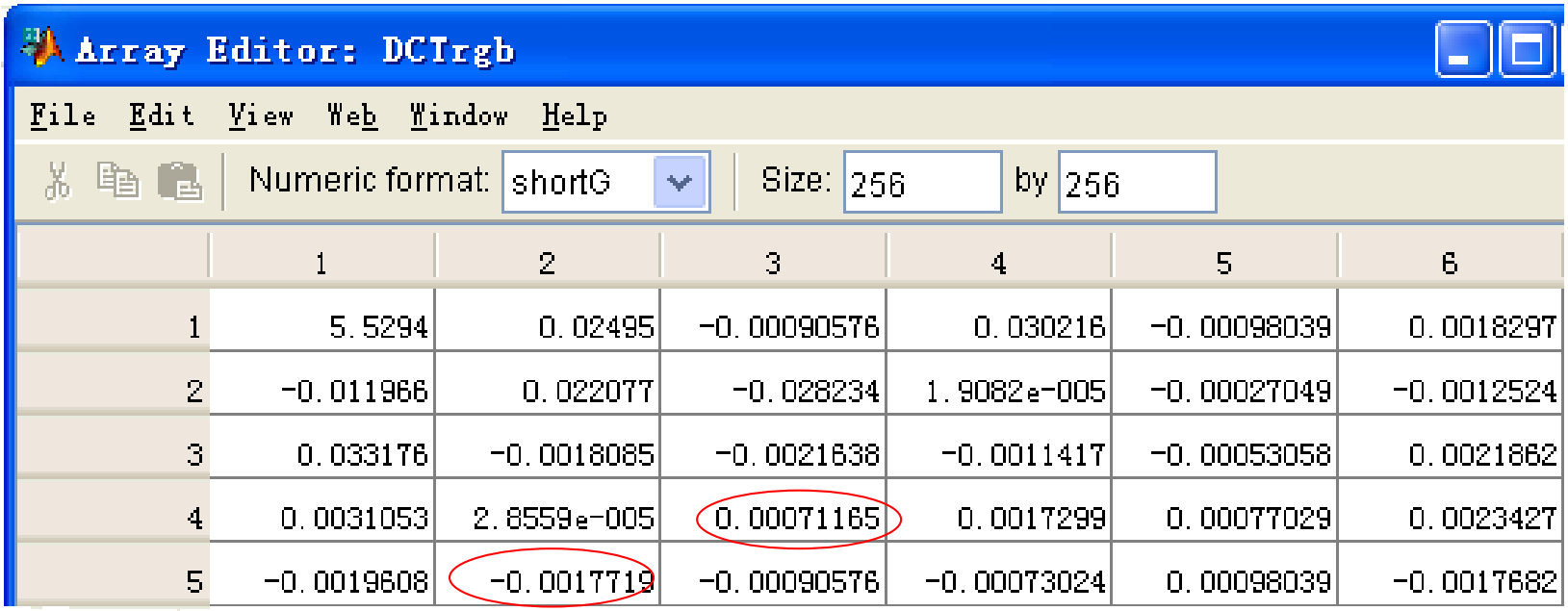
图像第一层的矩阵



	1	2	3	4	5	6
1	0.70196	0.69804	0.69804	0.70196	0.70196	0.69804
2	0.69804	0.69412	0.69412	0.69412	0.69804	0.69412
3	0.69804	0.69412	0.6902	0.6902	0.69412	0.6902
4	0.6902	0.68627	0.68235	0.68235	0.68627	0.68627
5	0.69804	0.6902	0.68235	0.68235	0.6902	0.6902
6	0.70196	0.6902	0.68627	0.68235	0.6902	0.6902

DCT域的信息隐秘

做分块DCT得到的矩阵



	1	2	3	4	5	6
1	5.5294	0.02495	-0.00090576	0.030216	-0.00098039	0.0018297
2	-0.011966	0.022077	-0.028234	1.9082e-005	-0.00027049	-0.0012524
3	0.033176	-0.0018085	-0.0021638	-0.0011417	-0.00053058	0.0021862
4	0.0031053	2.8559e-005	0.00071165	0.0017299	0.00077029	0.0023427
5	-0.0019608	-0.0017719	-0.00090576	-0.00073024	0.00098039	-0.0017682

DCT域的信息隐秘

隐藏信息前的DCT矩阵

Array Editor: DCTrgb0

File Edit View Web Window Help

Numeric format: shortG Size: 256 by 256

	1	2	3	4	5	6
1	5.5294	0.02495	-0.00090576	0.030216	-0.00098039	0.0018297
2	-0.011966	0.022077	-0.028234	1.9082e-005	-0.00027049	-0.0012524
3	0.033176	-0.0018085	-0.0021638	-0.0011417	-0.00053058	0.0021862
4	0.0031053	2.8559e-005	0.00071165	0.0017299	0.00077029	0.0023427
5	-0.0019608	-0.0017719	-0.00090576	-0.00073024	0.00098039	-0.0017682

DCT域的信息隐秘

隐藏信息后的DCT矩阵

Array Editor: DCTrgb

File Edit View Web Window Help

Numeric format: shortG Size: 256 by 256

	1	2	3	4	5	6
1	5.5294	0.02495	-0.00090576	0.030216	-0.00098039	0.0018297
2	-0.011966	0.022077	-0.028234	1.9082e-005	-0.00027049	-0.0012524
3	0.033176	-0.0018085	-0.0021638	-0.0011417	-0.00053058	0.0021862
4	0.0031053	2.8559e-005	-0.011772	0.0017299	0.00077029	0.0023427
5	-0.0019608	0.00071165	-0.00090576	-0.00073024	0.00098039	-0.0017682

DCT域的信息隐秘

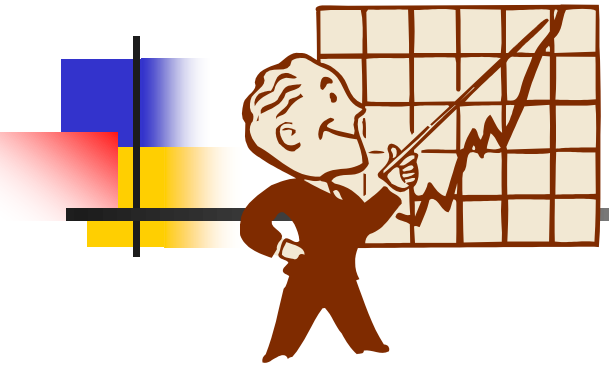
请注意比较上面两个表的（4，3）和（5，2）两个位置的数值，就可以看出我们对图像所做的处理。

第二部分

秘密信息的提取

DCT域的信息隐秘

既然是通过比较变换后的两个DCT系数来完成信息的隐藏，那么在传递秘密信息前，通信的双方就必须对要比较的两个位置达成一致，提取信息时接受者只需要获得载有秘密信息的图像，也对图像做DCT变换和分块，按照随机控制的顺序直接比较$B_i(u1,v1)$，$B_i(u2,v2)$的大小就能提取秘密信息了。



第三部分

对算法参数的讨论

DCT域的信息隐秘

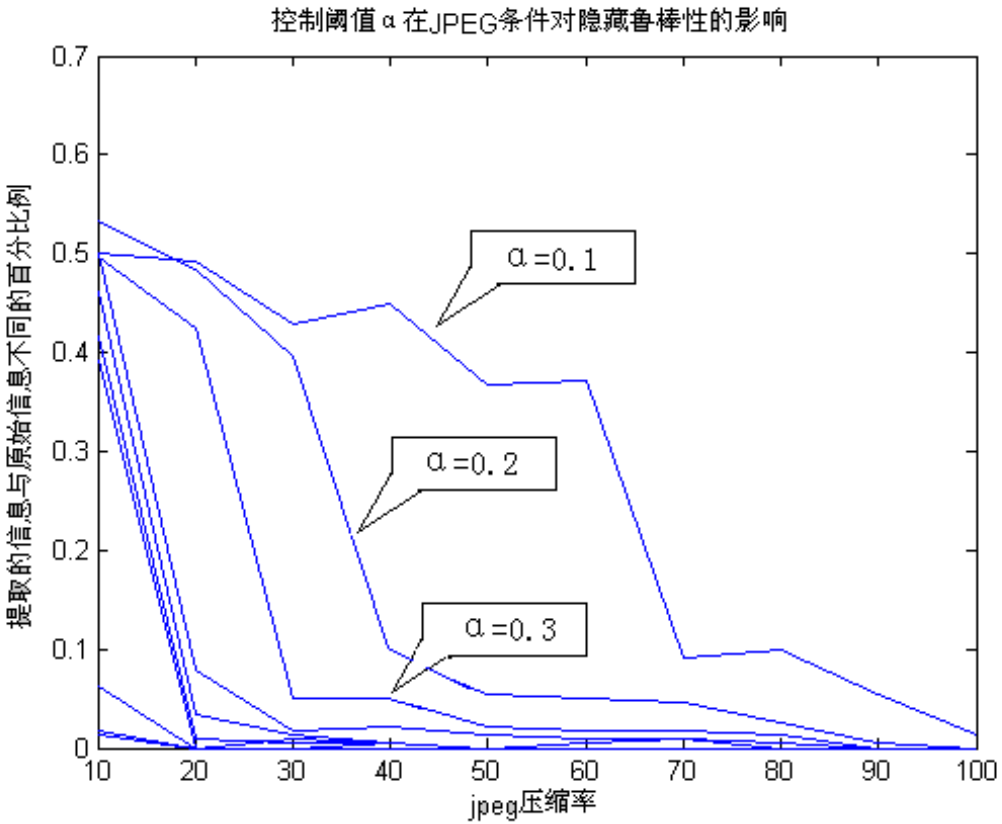
α是为了避免图像在传输过程中使$B_i(u1,v1)$和$B_i(u2,v2)$的相对大小发生错位从而使编码发生错误而引入的控制量，α越大，编码越不容易出错，图像的鲁棒性更强，但是α的取值的增大将带来载体视觉上的降质 。

DCT域的信息隐秘

1、α与隐藏鲁棒性的关系

我们以lenna.jpg为载体，秘密信息取为宋人宋祁的一句词句：“绿杨烟外晓寒轻，红杏枝头春意闹”。分别取不同α并对隐藏信息后的图像进行压缩。得到实验结果下图与下表。表是图的具体数据。

DCT域的信息隐秘


控制阈值α在JPEG条件对隐藏鲁棒性的影响
提取的信息与原始信息不同的百分比例
jpeg压缩率
α=0.1
α=0.2
α=0.3
0
0.1
0.2
0.3
0.4
0.5
0.6
0.7
10
20
30
40
50
60
70
80
90
100

DCT域的信息隐秘

	10%	20%	30%	40%	50%	60%	70%	80%	90%	100%
α=0.1	0.5	0.49167	0.42917	0.45	0.36667	0.37083	0.091667	0.1	0.054167	0.0125
α=0.2	0.53333	0.48333	0.39583	0.095833	0.054167	0.05	0.045833	0.025	0.0041667	0
α=0.3	0.49583	0.425	0.05	0.05	0.020833	0.016667	0.016667	0.0125	0	0
α=0.4	0.5	0.079167	0.016667	0.020833	0.0125	0.0083333	0.0083333	0.0041667	0	0
α=0.5	0.4625	0.033333	0.0125	0.0041667	0	0.0041667	0.0083333	0	0	0
α=0.6	0.41667	0.0083333	0.0041667	0.0041667	0	0	0	0	0	0
α=0.7	0.39167	0	0.0083333	0.0041667	0	0	0	0	0	0
α=0.8	0.0625	0	0	0.0041667	0	0	0	0	0	0
α=0.9	0.0125	0	0	0	0	0	0	0	0	0
α=1	0.016667	0	0	0	0	0	0	0	0	0

DCT域的信息隐秘

表中为数值为0，则表示其横向相应的α在纵向压缩率的条件下有强鲁棒性。数值不为0则表示相应的误码率，数值越大表示信息提取的越不真实。分析可见，α取0.1时，完全不能保证信息提取的正确。α在[0.2,0.4]区间内的抗JPEG压缩性能一般。当α取1时，基本可以认为是不受JPEG压缩干扰的。

DCT域的信息隐秘

下表是在对应于上一个表中加框（JPEG压缩率为50%）的列下实际信息提取的内容。可以发现，在α>0.3时，信息开始变得可读了。

DCT域的信息隐秘

原始信息	绿杨烟外晓寒轻，红杏枝头春意闹。
α=0.1	J　?鹳wF龒窩澌|??频颭碉掏蚿媢
α=0.2	聪盐烟下摸氷珥，簂杏R锻反阂饽
α=0.3	聪杨烟外晓寒玳，红杏露头春意闹。
α=0.4	绿杨烟外晓寒玑，红杏枝头春意闹。

DCT域的信息隐秘

α=0.5	绿杨烟外晓寒轻, 红杏枝头春意闹。
α=0.6	绿杨烟外晓寒轻, 红杏枝头春意闹。
α=0.7	绿杨烟外晓寒轻, 红杏枝头春意闹。

DCT域的信息隐秘

α=0.8	绿杨烟外晓寒轻, 红杏枝头春意闹。
α=0.9	绿杨烟外晓寒轻, 红杏枝头春意闹。
α=1	绿杨烟外晓寒轻, 红杏枝头春意闹。

DCT域的信息隐秘

2、α与隐藏不可见性的关系

给隐藏函数相同的入口参数（载体相同，信息相同，密钥相同），只取α不同，下面6幅图分别对应α的值为0.01，0.1，1，10，100，1000的情况，可以明显的看到随着α的值的增大，对图像的破坏越大。

DCT域的信息隐秘

α取为0.01

α取为0.1

DCT域的信息隐秘

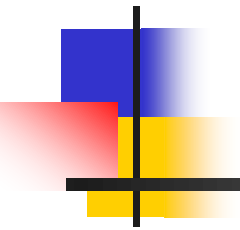
α取为1

α取为10

DCT域的信息隐秘

α取为100

α取为1000



小波域信息隐秘的讨论

小波域信息隐秘的讨论

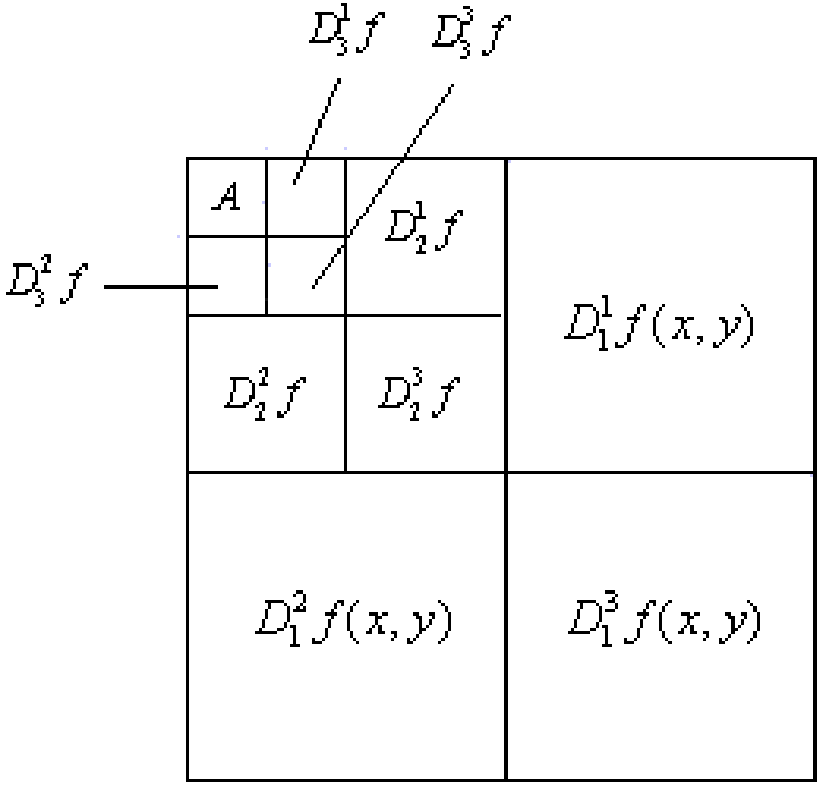
二维信号小波分解的Mallat算法可用下式描述：

$$A_{j-1}f(x,y)=A_j f(x,y)+D_j^1 f(x,y)+D_j^2 f(x,y)+D_j^3 f(x,y)$$

其中，j表示分解尺度，$\forall$为低频系数，D_j^1，D_j^2，D_j^3为j尺度下水平，垂直，对角方向上的三个高频系数。

小波域信息隐秘的讨论

二维信号的小波分解



小波域信息隐秘的讨论

关于小波域的信息隐秘，有几点需要说明一下：①二维小波分解的形态上图所示，低频分量居于左上角；②我们一般认为，将要隐藏的信息藏入低频系数会有较高的鲁棒性，但由于低频系数较少，嵌入信息的量有限，这就造成了鲁棒性与隐藏容量的矛盾；

小波域信息隐秘的讨论

③一种改进的设想是将信息藏入高尺度分解下的高频部分。做这种改进的原因是：a.这些部分仍然是一尺度下的低频部分，秘密信息隐藏在这些区域并不影响鲁棒性；b.将秘密信息隐藏在这些区域，隐藏的不可见性会比单纯隐藏在低频部分更好；c.这样可以扩大了隐藏信息的容量。