CSC 648 Project 1

Shuowen Wei

1.1 Below are the source codes of ***ecbImageEnc.m***

% ecbImageDec

% clc;clear

image\_name=input('Enter the image name to be decrypted -> ','s');

target=imread(image\_name);

if isempty(target)

sprintf('The image file %s does not exit!',image\_name);

break;

end

key=input('Enter key (0 - 255) -> ');

if ~isnumeric(key)

disp('Please input an interger key!');

break;

end

Output\_image=input('Enter output image name -> ','s');

ecb\_Image\_Dec=target;

figure;subplot(1,2,1);imshow(target);

title('the original image');

n=size(ecb\_Image\_Dec,1);

m=size(ecb\_Image\_Dec,2);

if (length(size(ecb\_Image\_Dec))==2)

for i=1:n

for j=1:m

a=uint8(ecb\_Image\_Dec(i,j));

b=uint8(mod(key+i+j-2,256));

ecb\_Image\_Dec(i,j)=bitxor(a,b);

end

end

else

for i=1:n

for j=1:m

a1=uint8(ecb\_Image\_Dec(i,j,1));

a2=uint8(ecb\_Image\_Dec(i,j,2));

a3=uint8(ecb\_Image\_Dec(i,j,3));

b=uint8(mod(key+i+j-2,256));

ecb\_Image\_Dec(i,j,1)=bitxor(a1,b);

ecb\_Image\_Dec(i,j,2)=bitxor(a2,b);

ecb\_Image\_Dec(i,j,3)=bitxor(a3,b);

end

end

end

pause(2);

subplot(1,2,2);imshow(ecb\_Image\_Dec);

title('the image decrypted by ECB');

imwrite(ecb\_Image\_Dec,Output\_image,'BMP');

An example as follows:

>> ecbImageEnc

Enter the image name to be encrypted -> lena.bmp

Enter key (0 - 255) -> 99

Enter output image name -> ecb\_lena\_Enc.bmp

1.2 Below are the source codes of ***ecbImageDec.m***

% ecbImageDec

% clc;clear

image\_name=input('Enter the image name to be decrypted -> ','s');

target=imread(image\_name);

if isempty(target)

sprintf('The image file %s does not exit!',image\_name);

break;

end

key=input('Enter key (0 - 255) -> ');

if ~isnumeric(key)

disp('Please input an interger key!');

break;

end

Output\_image=input('Enter output image name -> ','s');

ecb\_Image\_Dec=target;

figure;subplot(1,2,1);imshow(target);

title('the original image');

n=size(ecb\_Image\_Dec,1);

m=size(ecb\_Image\_Dec,2);

if (length(size(ecb\_Image\_Dec))==2)

for i=1:n

for j=1:m

a=uint8(ecb\_Image\_Dec(i,j));

b=uint8(mod(key+i+j-2,256));

ecb\_Image\_Dec(i,j)=bitxor(a,b);

end

end

else

for i=1:n

for j=1:m

a1=uint8(ecb\_Image\_Dec(i,j,1));

a2=uint8(ecb\_Image\_Dec(i,j,2));

a3=uint8(ecb\_Image\_Dec(i,j,3));

b=uint8(mod(key+i+j-2,256));

ecb\_Image\_Dec(i,j,1)=bitxor(a1,b);

ecb\_Image\_Dec(i,j,2)=bitxor(a2,b);

ecb\_Image\_Dec(i,j,3)=bitxor(a3,b);

end

end

end

pause(2);

subplot(1,2,2);imshow(ecb\_Image\_Dec);

title('the image decrypted by ECB');

imwrite(ecb\_Image\_Dec,Output\_image,'BMP');

An example as follows:

>> ecbImageDec

Enter the image name to be decrypted -> ecb\_lena\_Enc.bmp

Enter key (0 - 255) -> 99

Enter output image name -> ecb\_lena\_dec.bmp



2.1 Below are the source codes of ***cbcImageEnc.m***

% cbcImageEnc

% clc;clear

image\_name=input('Enter the image name to be encrypted -> ','s');

target=imread(image\_name);

if isempty(target)

sprintf('The image file %s does not exit!',image\_name);

break;

end

key=input('Enter key (0 - 255) -> ');

if ~isnumeric(key)

disp('Please input an interger key!');

break;

end

Output\_image=input('Enter output image name -> ','s');

cbc\_Image\_Enc=target;

figure;subplot(1,2,1);imshow(target);

title('the original image');

n=size(cbc\_Image\_Enc,1);

m=size(cbc\_Image\_Enc,2);

if(length(size(cbc\_Image\_Enc))==2)

for i=1:n

for j=1:m

a=uint8(cbc\_Image\_Enc(i,j));

b=uint8(mod(key+i+j-2,256));

if( (i==1)&&(j==1) )

cbc\_Image\_Enc(i,j)=bitxor(a,b);

c=cbc\_Image\_Enc(i,j);

else

d=bitxor(a,b);

cbc\_Image\_Enc(i,j)=bitxor(d,c);

c=cbc\_Image\_Enc(i,j);

end

end

end

else

for i=1:n

for j=1:m

a1=uint8(cbc\_Image\_Enc(i,j,1));

a2=uint8(cbc\_Image\_Enc(i,j,2));

a3=uint8(cbc\_Image\_Enc(i,j,3));

b=uint8(mod(key+i+j-2,256));

if( (i==1)&&(j==1) )

cbc\_Image\_Enc(i,j,1)=bitxor(a1,b);

cbc\_Image\_Enc(i,j,2)=bitxor(a2,b);

cbc\_Image\_Enc(i,j,3)=bitxor(a3,b);

c1=cbc\_Image\_Enc(i,j,1);

c2=cbc\_Image\_Enc(i,j,2);

c3=cbc\_Image\_Enc(i,j,3);

else

d1=bitxor(a1,b);

d2=bitxor(a2,b);

d3=bitxor(a3,b);

cbc\_Image\_Enc(i,j,1)=bitxor(d1,c1);

cbc\_Image\_Enc(i,j,2)=bitxor(d2,c2);

cbc\_Image\_Enc(i,j,3)=bitxor(d3,c3);

c1=cbc\_Image\_Enc(i,j,1);

c2=cbc\_Image\_Enc(i,j,2);

c3=cbc\_Image\_Enc(i,j,3);

end

end

end

end

pause(2);

subplot(1,2,2);imshow(cbc\_Image\_Enc);

title('the image encrypted by CBC');

imwrite(cbc\_Image\_Enc,Output\_image,'BMP');

An example as follows:

>> cbcImageEnc

Enter the image name to be encrypted -> lena.bmp

Enter key (0 - 255) -> 234

Enter output image name -> cbc\_lena\_Enc.bmp



2.2 Below are the source codes of ***cbcImageDec.m***

% cbcImageDec

% clc;clear

image\_name=input('Enter the image name to be decrypted -> ','s');

target=imread(image\_name);

if isempty(target)

sprintf('The image file %s does not exit!',image\_name);

break;

end

key=input('Enter key (0 - 255) -> ');

if ~isnumeric(key)

disp('Please input an interger key!');

break;

end

Output\_image=input('Enter output image name -> ','s');

cbc\_Image\_Dec=target;

figure;subplot(1,2,1);imshow(target);

title('the original image');

n=size(cbc\_Image\_Dec,1);

m=size(cbc\_Image\_Dec,2);

if(length(size(cbc\_Image\_Dec))==2)

for i=1:n

for j=1:m

a=uint8(cbc\_Image\_Dec(i,j));

b=uint8(mod(key+i+j-2,256));

if( (i==1)&&(j==1) )

c=cbc\_Image\_Dec(i,j);

cbc\_Image\_Dec(i,j)=bitxor(a,b);

else

d=bitxor(a,b);

prior\_c=cbc\_Image\_Dec(i,j);

cbc\_Image\_Dec(i,j)=bitxor(d,c);

c=prior\_c;

end

end

end

else

for i=1:n

for j=1:m

a1=uint8(cbc\_Image\_Dec(i,j,1));

a2=uint8(cbc\_Image\_Dec(i,j,2));

a3=uint8(cbc\_Image\_Dec(i,j,3));

b=uint8(mod(key+i+j-2,256));

if( (i==1)&&(j==1) )

c1=cbc\_Image\_Dec(i,j,1);

c2=cbc\_Image\_Dec(i,j,2);

c3=cbc\_Image\_Dec(i,j,3);

cbc\_Image\_Dec(i,j,1)=bitxor(a1,b);

cbc\_Image\_Dec(i,j,2)=bitxor(a2,b);

cbc\_Image\_Dec(i,j,3)=bitxor(a3,b);

else

d1=bitxor(a1,b);

d2=bitxor(a2,b);

d3=bitxor(a3,b);

prior\_c1=cbc\_Image\_Dec(i,j,1);

prior\_c2=cbc\_Image\_Dec(i,j,2);

prior\_c3=cbc\_Image\_Dec(i,j,3);

cbc\_Image\_Dec(i,j,1)=bitxor(d1,c1);

cbc\_Image\_Dec(i,j,2)=bitxor(d2,c2);

cbc\_Image\_Dec(i,j,3)=bitxor(d3,c3);

c1=prior\_c1;

c2=prior\_c2;

c3=prior\_c3;

end

end

end

end

pause(2);

subplot(1,2,2);imshow(cbc\_Image\_Dec);

title('the image decrypted by CBC');

imwrite(cbc\_Image\_Dec,Output\_image,'BMP');

An example as follows:

>> cbcImageDec

Enter the image name to be decrypted -> cbc\_lena\_Enc.bmp

Enter key (0 - 255) -> 234

Enter output image name -> cbc\_lena\_Dec.bmp

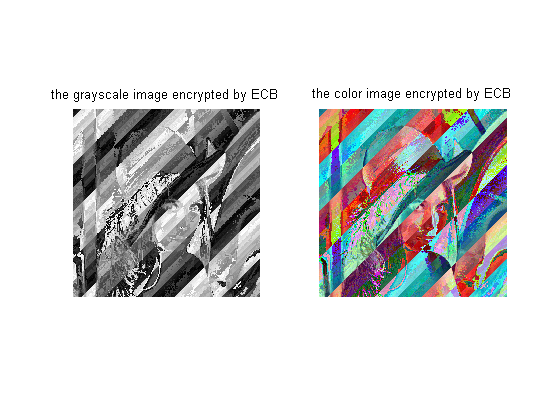


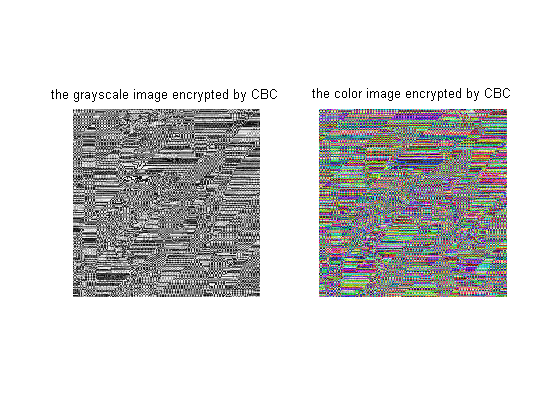
3.1

A: The images are listed above, and there is obviously a big visual difference between the images encrypted by ECB and CBC. The CBC encrypted image is much better than that of EBC in terms of protecting information because one basically can’t tell anything from the image after being encrypted by CBC, but it’s fairly easy to see the shape of Lena’s face and her hat in the ECB encrypted image. This is because of the different ways of how ECB and CBC processing the images. ECB only uses the key to compute the exclusive or on each individual pixel, while CBC operates not only the current pixel’s plaintext, but also combine the cipher of the last pixel, in which way it will have a bigger affluence on the original pixel than that by ECB.

3.2

A: The grayscale image read by Matlab is just a m-by-n matrix, while color image in Matlab is represented as m-by-n-by-3 matrix, basically the biggest difference of using the same method to encrypt grayscale and color image is that encrypting a grayscale image is much faster than processing color images. Results are showed below:





3.3

A: Yes, because the JPEG image is also represented as a m-by-n-by-3 matrix in Matlab, which is the same with the color BMP image, so my program works quite well. The results are showed below:

>> ecbImageEnc

Enter the image name to be encrypted -> Ronaldo.jpg

Enter key (0 - 255) -> 9

Enter output image name -> abc.jpg



>> cbcImageEnc

Enter the image name to be encrypted -> Ronaldo.jpg

Enter key (0 - 255) -> 9

Enter output image name -> def.jpg

