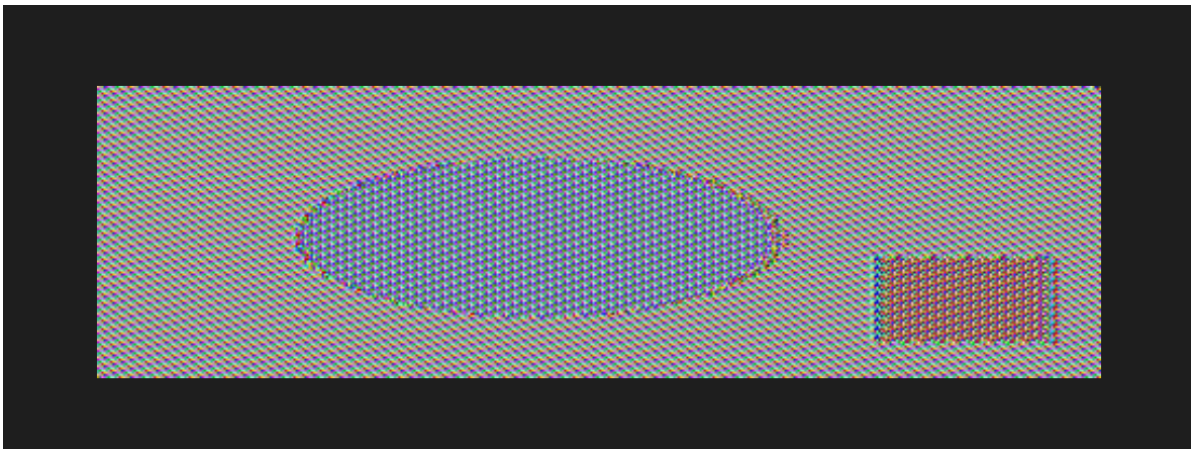
DotA Lab2-part3 report

3.1

I use AES-128 for image encryption.

For ECB algorithm:



The encrypted image is as above, and the pattern of original picture can still be figured out.

For CBC algorithm:

No pattern can be recognized from the encrypted image.

In conclusion, ECB algorithm only process information within same block, the relation between different blocks might still be inferred from the encrypted message, and thus is insecure.

3.2

The message to be encrypted is:

message.txt

```
How much information can you recover by decrypting a corrupted file, if the encryption mode
is ECB, CBC, CFB, or OFB, respectively?
```

I use a python script to run the four algorithm:

```
import subprocess
cypher_type = ['-aes-128-ecb', '-aes-128-cbc', '-aes-128-cfb', '-aes-128-ofb']
for tp in cypher_type:

    subprocess.run(['openssl', 'enc', '-e', tp, '-in', 'message.txt', '-out', 'encrypted.bin', '-K',
    bt = []
    with open('./encrypted.bin', 'rb') as file:
        bt = bytearray(file.read())
    bt[29] = 114
    with open('./corrupted.bin', 'wb') as file:
        file.write(bytes(bt))
    subprocess.run(['openssl', 'enc', '-d', tp, '-in', 'corrupted.bin', '-out', 'decrypted' + tp + '.
```

The result is as below:

- ECB:

  decrypted-aes-128-ecb.txt
  ```
  1  How much informa␛+␛iÖ␛␛F␛over by decrypting a corrupted file, if the encryption mode
  2  is ECB, CBC, CFB, or OFB, respectively?
  ```

  Only the block containing corrupted byte is damaged. This is because the independence of each block in ECB algorithm.

- CBC:

  decrypted-aes-128-cbc.txt
  ```
  1  How much informa)C␛8!␛ ␛a}␛␛qover by decry␛ting a corrupted file, if the encryption mode
  2  is ECB, CBC, CFB, or OFB, respectively?
  ```

  The corrupted block is only used for XOR operation on next block before encryption, and thus the value does not influence the subsequent encryption.

- CFB:

  decrypted-aes-128-cfb.txt
  ```
  1  How much information can you ␛ec␛qu␛␛[Z\v␛t␛␛␛ng a corrupted file, if the encryption mo
  2  is ECB, CBC, CFB, or OFB, respectively?
  ```

  Unlike the previous two algorithm, in CFB the sequential neighboring block is also corrupted. This is because a encrypted block is involved in the decryption of next block.

- OFB:

  decrypted-aes-128-ofb.txt
  ```
  1  How much information can you ␛ecover by decrypting a corrupted file, if the encryption mode
  2  is ECB, CBC, CFB, or OFB, respectively?
  ```

  Only the corrupted byte is damaged, since OFB does not encrypt blocks but encrypts IV and perform XOR operation on each block seperately.