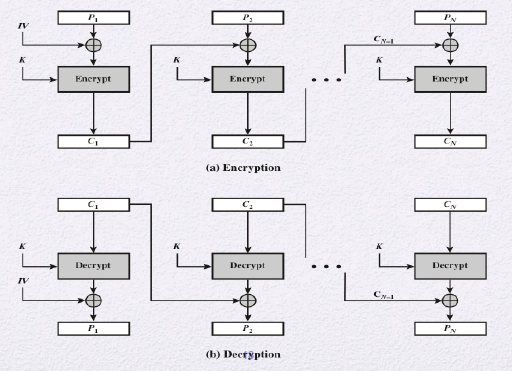
**Performance and Security Analysis Between AES and RNA-DNA Image Encryption**

* **CBC Mode and ECB Mode:**

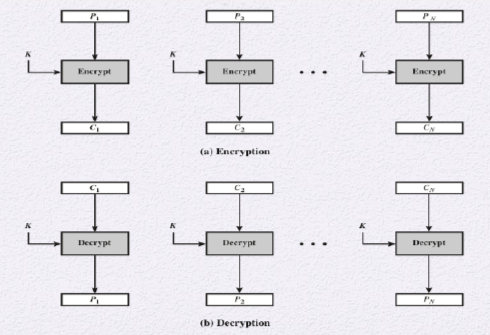
CBC (Cipher Block Chaining) Mode:

The input to the encryption algorithm is the XOR of the next block of plaintext and the preceding block of ciphertext.



ECB (Electronic Codebook) Mode:

Each block of plaintext bits is encoded independently using the same key.



* **Result:**

|  |  |  |  |
| --- | --- | --- | --- |
| Original (img10) | RNA-DNA | AES-CBC | AES-ECB |
| C:\Users\abcde\Desktop\Cryptography\project\image-encryption\new\image-encryption\Dataset\img_orig_gray10_cbc.png | C:\Users\abcde\Desktop\Cryptography\project\RNA-DNA-Image-Encryption\Dataset\10RNA.bmp | C:\Users\abcde\Desktop\Cryptography\project\image-encryption\Dataset\img_enc_gray10_cbc.png | C:\Users\abcde\Desktop\Cryptography\project\image-encryption\Dataset\img_enc_gray10_ecb.png |

|  |  |  |  |
| --- | --- | --- | --- |
| Original (img13) | RNA-DNA | AES-CBC | AES-ECB |
| C:\Users\abcde\Desktop\Cryptography\project\image-encryption\new\image-encryption\Dataset\img_orig_gray13_cbc.png | C:\Users\abcde\Desktop\Cryptography\project\RNA-DNA-Image-Encryption\Dataset\13RNA.bmp | C:\Users\abcde\Desktop\Cryptography\project\image-encryption\Dataset\img_enc_gray13_cbc.png | C:\Users\abcde\Desktop\Cryptography\project\image-encryption\Dataset\img_enc_gray13_ecb.png |

|  |  |  |  |
| --- | --- | --- | --- |
| Original (img17) | RNA-DNA | AES-CBC | AES-ECB |
| C:\Users\abcde\Desktop\Cryptography\project\image-encryption\new\image-encryption\Dataset\img_orig_gray17_cbc.png | C:\Users\abcde\Desktop\Cryptography\project\RNA-DNA-Image-Encryption\Dataset\17RNA.bmp | C:\Users\abcde\Desktop\Cryptography\project\image-encryption\Dataset\img_enc_gray17_cbc.png | C:\Users\abcde\Desktop\Cryptography\project\image-encryption\Dataset\img_enc_gray17_ecb.png |

|  |  |  |  |
| --- | --- | --- | --- |
| Original (img66) | RNA-DNA | AES-CBC | AES-ECB |
| C:\Users\abcde\Desktop\Cryptography\project\image-encryption\new\image-encryption\Dataset\img_orig_gray66_cbc.png | C:\Users\abcde\Desktop\Cryptography\project\RNA-DNA-Image-Encryption\Dataset\66RNA.bmp | C:\Users\abcde\Desktop\Cryptography\project\image-encryption\Dataset\img_enc_gray66_cbc.png | C:\Users\abcde\Desktop\Cryptography\project\image-encryption\Dataset\img_enc_gray66_ecb.png |

1. **Statistical Analysis**
2. Histogram (provide any clue to employ any statistical analysis attack on the encryption image)

|  |  |  |
| --- | --- | --- |
| RNA-DNA | AES-CBC | AES-ECB |
| C:\Users\abcde\Desktop\Cryptography\project\RNA-DNA-Image-Encryption\10.png | C:\Users\abcde\Desktop\Cryptography\project\image-encryption\new\image-encryption\Dataset\img_hist10_cbc.png | C:\Users\abcde\Desktop\Cryptography\project\image-encryption\new\image-encryption\Dataset\img_hist10_ecb.png |

|  |  |  |
| --- | --- | --- |
| RNA-DNA | AES-CBC | AES-ECB |
| C:\Users\abcde\Desktop\Cryptography\project\RNA-DNA-Image-Encryption\13.png | C:\Users\abcde\Desktop\Cryptography\project\image-encryption\new\image-encryption\Dataset\img_hist13_cbc.png | C:\Users\abcde\Desktop\Cryptography\project\image-encryption\new\image-encryption\Dataset\img_hist13_ecb.png |

|  |  |  |
| --- | --- | --- |
| RNA-DNA | AES-CBC | AES-ECB |
| C:\Users\abcde\Desktop\Cryptography\project\RNA-DNA-Image-Encryption\17.png | C:\Users\abcde\Desktop\Cryptography\project\image-encryption\new\image-encryption\Dataset\img_hist17_cbc.png | C:\Users\abcde\Desktop\Cryptography\project\image-encryption\new\image-encryption\Dataset\img_hist17_ecb.png |

|  |  |  |
| --- | --- | --- |
| RNA-DNA | AES-CBC | AES-ECB |
| C:\Users\abcde\Desktop\Cryptography\project\RNA-DNA-Image-Encryption\66.png | C:\Users\abcde\Desktop\Cryptography\project\image-encryption\new\image-encryption\Dataset\img_hist66_cbc.png | C:\Users\abcde\Desktop\Cryptography\project\image-encryption\new\image-encryption\Dataset\img_hist66_ecb.png |

1. Correlation Analysis of Two Adjacent Pixels

Correlation Analysis of Ciphered Image

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Image | | Horizontal | Vertical | Diagonal |
| 10 | RNA-DNA | -0.0069 | -0.002 | 0.0183 |
| AES (CBC) | 0.0213 | -0.0143 | -0.0071 |
| AES (ECB) | 0.0261 | 0.0346 | 0.0721 |
| 13 | RNA-DNA | 0.0111 | -0.0276 | -0.0026 |
| AES (CBC) | -0.0044 | 0.0008 | 0.0061 |
| AES (ECB) | 0.4743 | -0.2188 | -0.2159 |
| 17 | RNA-DNA | 0.0027 | 0.0163 | 0.0016 |
| AES (CBC) | 0.0041 | -0.0044 | 0.0058 |
| AES (ECB) | 0.6981 | -0.3189 | -0.3115 |
| 66 | RNA-DNA | 0.0072 | -0.0088 | -0.006 |
| AES (CBC) | 0.0079 | -0.0115 | -0.0015 |
| AES (ECB) | 0.0156 | -0.0355 | 0.0014 |

From top to down, show the correlation analysis result of image 10, 13, 17, 66, respectively.

|  |  |  |
| --- | --- | --- |
| RNA-DNA | AES-CBC | AES-ECB |
| C:\Users\abcde\Desktop\Cryptography\project\RNA-DNA-Image-Encryption\Dataset\10DiagonalCorPlt.png | C:\Users\abcde\Desktop\Cryptography\project\image-encryption\Dataset\img_cor_diagonal10_cbc.png | C:\Users\abcde\Desktop\Cryptography\project\image-encryption\Dataset\img_cor_diagonal10_ecb.png |
| C:\Users\abcde\Desktop\Cryptography\project\RNA-DNA-Image-Encryption\Dataset\13DiagonalCorPlt.png | C:\Users\abcde\Desktop\Cryptography\project\image-encryption\Dataset\img_cor_diagonal13_cbc.png | C:\Users\abcde\Desktop\Cryptography\project\image-encryption\Dataset\img_cor_diagonal13_ecb.png |
| C:\Users\abcde\Desktop\Cryptography\project\RNA-DNA-Image-Encryption\Dataset\17DiagonalCorPlt.png | C:\Users\abcde\Desktop\Cryptography\project\image-encryption\Dataset\img_cor_diagonal17_cbc.png | C:\Users\abcde\Desktop\Cryptography\project\image-encryption\Dataset\img_cor_diagonal17_ecb.png |
| C:\Users\abcde\Desktop\Cryptography\project\RNA-DNA-Image-Encryption\Dataset\66DiagonalCorPlt.png | C:\Users\abcde\Desktop\Cryptography\project\image-encryption\Dataset\img_cor_diagonal66_cbc.png | C:\Users\abcde\Desktop\Cryptography\project\image-encryption\Dataset\img_cor_diagonal66_ecb.png |

1. **Sensibility Analysis**
2. Differential Attack(NPCR、UACI)

Image 10

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  |  | RNA-DNA | AES-CBC | AES-ECB |
| NPCR | RUN 1 | 0.997847 | 0.997847 | 0.997985 |
| RUN 2 | 0.995477 | 0.997985 | 0.997985 |
| RUN 3 | 0.99917 | 0.997906 | 0.997985 |
| Average | 0.997498 | 0.997913 | 0.997985 |
| UACI | RUN 1 | 0.328285 | 0.368189 | 0.369524 |
| RUN 2 | 0.340357 | 0.368879 | 0.369524 |
| RUN 3 | 0.326552 | 0.367884 | 0.369516 |
| Average | 0.331732 | 0.368317 | 0.369521 |

Image 13

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  |  | RNA-DNA | AES-CBC | AES-ECB |
| NPCR | RUN 1 | 0.995152 | 0.998138 | 0.998154 |
| RUN 2 | 0.997524 | 0.998085 | 0.998154 |
| RUN 3 | 0.995728 | 0.998096 | 0.998154 |
| Average | 0.996134 | 0.998107 | 0.998154 |
| UACI | RUN 1 | 0.334364 | 0.400719 | 0.425438 |
| RUN 2 | 0.340444 | 0.400252 | 0.425441 |
| RUN 3 | 0.338779 | 0.400246 | 0.425442 |
| Average | 0.337862 | 0.400406 | 0.42544 |

Image 17

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  |  | RNA-DNA | AES-CBC | AES-ECB |
| NPCR | RUN 1 | 0.995155 | 0.998749 | 0.998787 |
| RUN 2 | 0.99667 | 0.998783 | 0.998787 |
| RUN 3 | 0.995987 | 0.998848 | 0.998787 |
| Average | 0.995937 | 0.998793 | 0.998787 |
| UACI | RUN 1 | 0.334364 | 0.438207 | 0.472142 |
| RUN 2 | 0.340444 | 0.438276 | 0.472145 |
| RUN 3 | 0.338779 | 0.437886 | 0.472146 |
| Average | 0.337862 | 0.438123 | 0.472145 |

Image 66

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  |  | RNA-DNA | AES-CBC | AES-ECB |
| NPCR | RUN 1 | 0.997239 | 0.994637 | 0.993763 |
| RUN 2 | 0.995551 | 0.99412 | 0.993763 |
| RUN 3 | 0.994736 | 0.994696 | 0.993763 |
| Average | 0.995842 | 0.994485 | 0.993763 |
| UACI | RUN 1 | 0.333569 | 0.227215 | 0.224651 |
| RUN 2 | 0.339571 | 0.227923 | 0.224652 |
| RUN 3 | 0.339571 | 0.225827 | 0.224658 |
| Average | 0.332441 | 0.226988 | 0.224653 |

1. Information Entropy Analysis

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | Original | RNA-DNA | AES-CBC | AES-ECB |
| Image 10 | 6.19884089341 | 7.99617046439 | 7.63783426615 | 7.54539756786 |
| Image 13 | 4.02843345403 | 7.99929526227 | 7.63878294346 | 6.40051673297 |
| Image 17 | 2.64166441471 | 7.99930342855 | 7.63785855258 | 5.57253834808 |
| Image 66 | 7.08471964285 | 7.99625431755 | 7.63612423939 | 7.63425886866 |

1. Time Analysis

|  |  |  |  |
| --- | --- | --- | --- |
|  | RNA-DNA | AES-CBC | AES-ECB |
| Image 10 | 2.826 | 0.005 | 0.011 |
| Image 13 | 14.927 | 0.008 | 0.012 |
| Image 17 | 14.883 | 0.017 | 0.007 |
| Image 66 | 2.977 | 0.003 | 0.008 |