Image encryption by AES algorithm based on Chaos-Permutation

*Rachid RIMANI*, Naima HADJ SAID, Adda ALI-PACHA, Juan Antonio López RAMOS

*a* University Mustapha, Stambouli of MASCARA, LACOSI Laboratory, ALGERIA  
b, c University of Sciences and Technology of Oran Mohamed Boudiaf USTOMB – ALGERIA  
d Department of Mathematics, University of Almeria, SPAIN

*Corresponding author: rachid.rimani@univ-usto.dz*

Received: 17/06/2019, Accepted: 21/10/2019

Abstract

Today, in particular with the development of the internet, transmitting confidential information in a secure manner has become a basic need; data encryption is often the only effective way to meet these requirements. Traditional cryptography is the study of methods for transmitting confidential data; in modern cryptography, transformation is applied to the plain message that makes it incomprehensible: these transformations are mathematical functions, called cryptographic algorithms, which depend on a parameter called key. In this paper, we presents a new symmetrical crypto-system by block for encrypting images on using the encryption AES algorithm (Advanced Encryption Standard) combined with the CBC mode (Cipher Block Chaining) in order to improve the security level. The proposed crypto-system consists on replacing the linear permutation of ShiftRows step of the AES encryption algorithm by a nonlinear and random permutation, this permutation is calculated by a chaotic sequel.

Keywords: AES algorithm, chaotic sequel, encrypting images, non-linear permutation, random permutation, symmetrical cryptosystem.

Introduction

Cryptography is a mathematical technique that allows the transmission of confidential data on an unsecured medium without an intruder discovering the content. These data will be decrypted only by the recipient or the one knowing the encryption key. Cryptography guarantees, among other things, integrity, non-repudiation and the authenticity of the data in addition to confidentiality (Menezes et al, 1997); currently, several cryptographic systems have emerged to solve new security issues such as access to information, communications between computers, and e-commerce.

Encryption algorithms can be separated according to the encryption technique in two main categories: per block or per stream. Block cipher is the most appropriate for encrypting images because of their size and their information which is two-dimensional in nature and at times redundant. Therefore, we use the block cipher in our crypto-system.

The iterative encryption algorithms by block are essentially divided into two major structures. According to the architecture of the internal iteration function, the two mainly used structures are: the Feistel scheme (used in DES and RC6), and substitution-permutation network structure SPN (used in AES). In addition, each structure can be fixed (fixed key for each iteration) or variable (dynamic key with iterations). It is clear that the variable structure that depends on the iteration keys is more difficult to study by the attacker, and for this reason, we adopt it for the proposed crypto-system.
In order to build a secure encryption system, Shannon (1949) set out two fundamental principles to respect, which are confusion and diffusion. Confusion is provided by a nonlinear substitution, and the diffusion technique is often realized by the permutations of blocks, pixels or binary permutations (Yanbing et al, 2012; Schneier, 1996). Examples of algorithms that apply permutations are various, we quote DES, AES, and RC4 (RSA, 2003). We introduced in this paper a new permutation technique to ensure the diffusion, whose principle is to replace the linear permutation of ShiftRows step of the AES encryption algorithm by a nonlinear and random permutation, which varies according to the chaotic sequel already generated. The use of the CBC mode allows to guarantee that even if the gross image contains many identical blocks, each of them will be encrypted differently.

Structure of AES

The AES (Advanced Encryption Standard) is a symmetric encryption algorithm that processes data blocks of 128, 196 or 256 bits and the size of the typically key used is 128 bits with variants of 192 and 256 bits (Daemen & Rijmen, 2002; Stallings (2011). The data blocks and the key are stored in a table as shown in Figure 1; the number of columns depends on the blocks size and the key.

![Figure 1. State table block](image)

AES is based on a succession of rounds; the number of rounds varies depending on the block size and the key size according to the Table 1.

| |K| =128 | |K| =192 | |K| =256 |
|---|---|---|---|
| |B| =128 | 10 | 12 | 14 |
| |B| =192 | 12 | 12 | 14 |
| |B| =256 | 14 | 14 | 14 |

where |K| : Key size ; |B| : block size.

In our case, we will use the AES algorithm for a 128 bits block size with a 128 bits key size also giving a number of rounds r equal to 10. The AES algorithm in the encryption mode consists of 3 steps:
a. The first is an " exclusive or" operation between the plaintext block and the secret key K.
b. The second step is a set of 9 rounds each executing 4 operations: SubBytes, ShiftRows, MixColumns and AddRoundKey.
c. The last step is a round in which the MixColumns operation is not performed.

All the encryption operations are invertible. Therefore, in order to decrypt a block, we apply operations reversely.
Contribution: Image Encryption By AES Algorithm With Chaos-Permutation

Images encryption is provided by the AES algorithm replacing the permutation of ShiftRows step by the permutation table obtained using a logistic map method (logistic chaos of parameter $\mu$, $X0$ and $F$) to generate a sequence $st$ of pseudorandom numbers without repetition modulo (depending on key size) as shown in Figure 2 and Figure 3.

\[
\begin{array}{ccc}
\mu & X0 & F \\
3.967 & 0.19 & 5 \\
\end{array}
\]

Set parameters $\mu$, $X0$, $F$,

Calculate the logistic map of the pseudo random numbers modulo 6

Find the permutation $st$

| 4 | 6 | 8 | 1 | 7 | 2 | 5 | 15 | 9 | 12 | 14 | 8 | 10 | 13 | 16 | 11 |

Encryption/decryption using of the permutation table

The recipient must calculate the permutation $st$ using the same shared parameters $\mu$, $X0$ and $F$ to have the permutation table; so to decrypt a block, the same procedure is applied reversely. When the image contains homogeneous areas, all identical blocks will also be identical after encryption. In this case, the ciphered image contains textured areas and the entropy of the image is not maximal. To solve this problem, we applied the CBC mode on our
algorithm; this allows on one hand to increase the level of complexity and on the other hand satisfies second Shannon’s theory of diffusion.

Security Analysis of Proposed Crypto-System and Experimental Results

After the encryption of an image, we must have an independence (low correlation) between the original image pixels and that of the ciphered image. This independence can be seen by simple viewing of the ciphered image, but the visual inspection remains insufficient to judge the encryption of an image. The metrics for evaluating the degree of encryption can be classified into statistical analysis, differential analysis and sensitivity analysis of the secret key.

Statistical analysis

To resist the statistical attack, the histogram of the ciphered image must be very close to a uniform distribution (Figure 4.e). To measure this uniformity, we apply two tests, the first test is chi-square and the second test is entropy.

A. Chi-Square test

The chi-square test is given by the following relation:
The distribution of the histogram is uniform if it satisfies the following condition:

\[ X_{\text{exp}}^2 < X_{\text{th \ 0.05}}^2 = 273.12 \]

for a threshold \( \alpha \) fixed at 0.05 in our experiment. In our case we found \( X_{\text{exp}}^2 = 259.7449 \).

**B. Entropy test**

The entropy test of an image \( M \) is given by equation 2:

\[ H(M) = \sum_{i=0}^{Q-1} p_i \log_2 \left( \frac{1}{p_i} \right) = -\sum_{i=0}^{Q-1} p_i \log_2 p_i \] (2)

In the case of a uniform distribution, the entropy \( H(M) \) is maximum and is given by equation 3:

\[ H_{\text{max}} = \log_2 (Q) = 8 \] (3)

Thus, if the value of entropy is very close to \( H_{\text{max}} \), it means that the source data has a nearly uniform distribution and the crypto-system providing such data can withstand the statistical attack.

Figure 4 shows the results of Lena's image 224x224, encrypted by the AES algorithm with Chaos-Permutation in CBC mode.

We notice that the ciphered image is not visible anymore. Comparing the plain image histogram with the ciphered image histogram, we note that the occurrence probabilities of each gray level are uniformly distributed with a very high entropy of ciphered image (close to 7.9963).
Table 2 indicates that the entropy of the AES algorithm with Chaos-Permutation is large compared to the AES algorithm; we also note that the entropy of the AES algorithm with Chaos-Permutation in CBC mode is high compared to the algorithm without CBC mode, so we can say that we have added complexity by CBC mode.

**Table 2. Comparison of entropy between AES encryption algorithm and Chaos-permutation with and in CBC mode**

<table>
<thead>
<tr>
<th>Algorithm</th>
<th>Entropy Plain</th>
<th>Entropy Cipher</th>
</tr>
</thead>
<tbody>
<tr>
<td>AES in CBC mode</td>
<td>7.2353</td>
<td>7.9961</td>
</tr>
<tr>
<td>Chaos-Permutation in CBC mode</td>
<td>==</td>
<td>7.9963</td>
</tr>
</tbody>
</table>

**C. Correlation coefficient of adjacent pixels**

The calculation of the correlation coefficient between the pixels allows evaluating the encryption quality of cryptosystem. Generally, in an original image, each pixel is strongly correlated with its adjacent pixels in the three directions horizontal, vertical and diagonal. An ideal cryptosystem should produce encrypted images without any correlation between adjacent pixels. To test the correlation between adjacent pixels; we took 5300 pairs of two adjacent pixels from the original image and those encrypted in the three directions horizontal, vertical and diagonal as follows:

For each selected pixel (at the number 5300) of coordinates \((i, j)\) we form 4 vectors \(V, V_H, V_V, V_D\) containing the gray levels of the pixels which are found at the positions \((i, j), (i+1, j), (i, j+1), (i+1, j+1)\) respectively. The correlation coefficients in the three directions are \(C_{VH}, C_{VV}, C_{VD}\).

Table 3 groups the correlation coefficients for the following algorithms: the proposed algorithm AES with Chaos-Permutation, ECKBA proposed in (Socek et al., 2005) (it was cited and described as references for several proposals of image encryption algorithm (Awad et al., 2008; El-Waled, et al., 2008, Noura et al., 2011; Philip et al., 2011) and the algorithm proposed by Mansour et al (2012). We notice that the correlation coefficients measured for the original image are close to 1, while the correlation coefficients for the encrypted images of different algorithms are close to 0, it is also deduced that the encryption has considerably attenuated the correlation between pixels of encrypted images.

**Table 3. Correlation coefficient of adjacent pixels**

<table>
<thead>
<tr>
<th>Direction</th>
<th>HORIZONTAL</th>
<th>VERTICAL</th>
<th>DIAGONAL</th>
</tr>
</thead>
<tbody>
<tr>
<td>Plain image</td>
<td>0.9244</td>
<td>0.9588</td>
<td>0.8948</td>
</tr>
<tr>
<td>Chaos-Permutation</td>
<td>-0.0021</td>
<td>0.0143</td>
<td>0.0085</td>
</tr>
<tr>
<td>ECKBA</td>
<td>0.0760</td>
<td>0.0227</td>
<td>-0.0012</td>
</tr>
<tr>
<td>Mansour et al</td>
<td>0.0479</td>
<td>-0.0414</td>
<td>-0.0416</td>
</tr>
</tbody>
</table>

In order to compare the performances of the proposed algorithm with ECKBA and Mansour et al algorithm, we have plotted the graph in Figure 5, which represents in absolute value the correlation coefficients of the adjacent pixels of the encrypted images of each algorithm.

We note that for the horizontal and vertical direction, Chaos-Permutation performance has exceeded the other two algorithms; with the exception of the ECKBA algorithm which has a value of diagonal adjacent pixels lower than the proposed algorithm.
Figure 5. Correlation coefficient comparison of adjacent pixels for different algorithms

Figure 6 represents the correlation distributions of the horizontal, vertical and diagonal adjacent pixels in the original image. We note that the pixel intensity distribution is focused on the diagonal; the pixels are then strongly correlated.

Figure 6. Correlation distribution of peers of adjacent pixels in the original image: a) Horizontally, b) Vertically, c) Diagonally

Figure 7 represents the correlation distributions of the horizontal, vertical and diagonal adjacent pixels in the encrypted image. We note that the pixel intensity distributions are uncorrelated and they have a uniform distribution.

Figure 7. Correlation distribution of peers of adjacent pixels in the encrypted image: a) Horizontally, b) Vertically, c) Diagonally

All results show that the crypto-system used reveals good properties and resists against statistical attacks.

Differential analysis

To ensure the security of an image encryption scheme against differential analysis, two quantitative measures are used: the Number of Pixels Change Rate (NPCR) and the Unified Average Changing Intensity (UACI) defined by the following equation:
Table 4. NPCR and UACI values between the original image and the encrypted image

<table>
<thead>
<tr>
<th>Algorithm</th>
<th>NPCR (%)</th>
<th>UACI (%)</th>
</tr>
</thead>
<tbody>
<tr>
<td>AES</td>
<td>99.5556</td>
<td>15.2373</td>
</tr>
<tr>
<td>Chaos-Permutation</td>
<td>99.6293</td>
<td>15.4133</td>
</tr>
<tr>
<td>ECKBA</td>
<td>99.5625</td>
<td>13.4146</td>
</tr>
<tr>
<td>Mansour et al</td>
<td>99.5937</td>
<td>13.0731</td>
</tr>
</tbody>
</table>

We performed another test between two encrypted images (LENA 224*224) that differ from the original image by a single pixel, the NPCR and UACI values are shown in Table 5.

Table 5. NPCR and UACI values between two encrypted images with one pixel different at the origin

<table>
<thead>
<tr>
<th>Algorithm</th>
<th>NPCR (%)</th>
<th>UACI (%)</th>
</tr>
</thead>
<tbody>
<tr>
<td>AES</td>
<td>0.0319</td>
<td>0.0091</td>
</tr>
<tr>
<td>Chaos-Permutation</td>
<td>0.0319</td>
<td>0.0104</td>
</tr>
<tr>
<td>Chaos-Permutation in CBC mode</td>
<td>56.1683</td>
<td>18.8875</td>
</tr>
<tr>
<td>ECKBA</td>
<td>100</td>
<td>15.9849</td>
</tr>
<tr>
<td>Mansour et al</td>
<td>0.0156</td>
<td>0.0059</td>
</tr>
</tbody>
</table>

Note that we have obtained the same NPCR compared to the AES algorithm, but the UACI value by the algorithm the Chaos-Permutation in CBC mode is the best. We also note that the NPCR of the ECKBA algorithm reaches the maximum value but its UACI value remains lower than the proposed algorithm.

Sensitivity of the Secret Key

To test the sensitivity of the key on our crypto-system and therefore the reliability of the proposed approach; we did two different tests:

a. The first test is to encrypt the same image by two keys slightly different; the used keys are different only by a single bit at the initial condition.

K1=[9 17 43 74;36 20 85 13;41 7 16 54;21 47 63 95] 01011111
K2=[9 17 43 7 4;36 20 85 13;41 7 16 54;21 47 63 31] 00011111
Figure 8 contains the histograms of Lena’s image (224x224) encrypted by the two keys K1 and K2.

![Histograms of Lena’s image encrypted by K1 and K2](image)

**Figure 8.** Image encrypt by two slightly different keys K1 and K2

a) Plain image  
b) Ciphered image with K1,  
c) Histogram of image (b),  
d) Ciphered image with K2,  
e) Histogram of image (d)

Changing a single bit in the encryption key then gives two completely different histograms with a very low correlation coefficient between the two encrypted images (corrcoef = 0.0080). Therefore, the two encrypted images are completely independent from each other.

b. The second test consists on using the key K1 to encrypt an image (LENA 80x80), and using the key K2 in the decryption phase (Figure 9).

![Images of decrypted images](image)

**Figure 9.** a) Plain image, b) Image decrypted by K2, c) Image decrypted by K1

We notice that the decryption process failed when the secret key is slightly changed and the decrypted image is completely blurred (Figure 9.b).

With these two tests, we conclude that the AES algorithm with Chaos-Permutation is extremely sensitive to small changes of the secret key, so we can say that the proposed approach guarantees security against brute force attacks.

**Avalanche Criterion**

Any function that satisfies this criterion must have a change with a probability of one-half of the output bits, if only one bit at the input changes. The output will then be uniform and no statistical prediction can take place (Adams & Tavares, 1989; Rohiem et al., 2005; Webster & Tavares, 1998; Benjeddou, 2008).

**Calculation of the Hamming distance**

The Hamming distance is the number of different bits between two binary sequences C1 and C2, which will be noted $d_H(C1, C2)$. This criterion measures the avalanche effect and it is defined by the equation 6:
We encrypted two binary sequences $E_1$ and $E_2$, which differ by a single bit by our algorithm AES with ChaosPermutation, then we calculated the Hamming distance between the two resulting encrypted sequences $C_1$ and $C_2$, by changing each time the position of the bit to be changed for plain text sequences. Figure 10 shows the percentage of the Hamming distance in bits given by equation 7:

$$d_H(C_1, C_2) = \sum_{i=0}^{n-1} |C_1(i), C_2(i)|$$  \hspace{1cm} (6)$$

The size of the binary sequences tested is $L_b = 128$ bits and $j$ represents the different bit position. We obtain 78.91% pairs of encrypted sequences with a Hamming distance greater than 46%, and 21.09% pairs having a distance less than 46%; the average value of the Hamming distance obtained for our algorithm is 49.6338 (Figure 10); indeed whatever the position of the changed bit, this provided almost 50% of difference between the bits of two concerned sequences. So we can say that the avalanche property is reached by the algorithm AES with Chaos-Permutation.

Figure 10. Percentage in bits of the Hamming distance according to the positions of the changed bits for pairs of encrypted texts by AES Chaos-Permutation

Conclusion

We have introduced in this work a new crypto-system in order to replace the linear permutation of the ShiftRows step with a random and nonlinear permutation. Another drawback in ShiftRows step is the public permutation; on the other hand, in the proposed approach, the permutation procedure is secret; this means that the security in the Chaos-Permutation method is not based on the encryption scheme, but on the confidentiality of shared parameters $F, \mu$ and $X_0$ of the logistic map.

For the chaos, the logistic map was used as an example for generating a pseudo random numbers, but if necessary, we look for another card, which will have best properties such as PWLCM.

The proposed algorithm is suitable for images, audio, text; and if we change the size of the bloc, the encryption/ decryption procedure does not change; it is sufficient to modify the size of the permutation table.

In conclusion, we can say that the modification made on the AES algorithm does not have any influence in its efficiency, but also enhances its fortress as can be observed in the entropy and other values obtained.
References