An Improved AES Encryption Algorithm Based on the Hénon and Chebyshev Chaotic Map

Yufen FENG*1, Yubin LIU2, Guangfeng ZHAO3, Mingna XIA*4

1. Department of Mathematics and Information Science, Tangshan Normal University, Tangshan, 063000, China
2. Department of Computer Science, Tangshan Normal University, Tangshan, 063000, China
3. Research Department, Tangshan Normal University, Tangshan, 063000, China
4. Tangshan Vocational & Technical College, No.120 Xinhua West Road, Tangshan, 063004, China

Abstract — Aimed at the problems of poor security existing in the conventional Advanced Encryption Standard (AES) algorithm, the paper presents an improved AES algorithm based on the two-dimensional Hénon and Chebyshev chaotic map which can generate an independent round key randomly. The improved algorithm overcomes the disadvantage of the initial key is unchanged in the whole encryption process using the conventional AES algorithm. The experimental results show that the improved algorithm has a more reliable security than the conventional AES algorithm.

Keywords - AES algorithm, two-dimensional Hénon map, two-dimensional Chebyshev map, Image Encryption

I. INTRODUCTION

AES[1] (Advanced Encryption Standard) is an iterative and symmetric key password. The Rijndael algorithm designed by Belgian Joan Daemen and Vincent Rijmen became the new encryption standard AES(Advanced Encryption Standard) on October, 2000. It had replaced the DES (Data Encryption Standard) algorithm used more than 20 years to protect the sensitive information of the U.S. federal government.

The key is expanded by the seed key, a seed key information can also be deduced by the round key information, that is to say, as long as a round key is attacked, a seed key can be deduced by the mathematical model[2]. More over the initial key length of the AES algorithm round key is filled with the seed key directly, when the leakage of key information reaches a certain level, the seed key can be obtained by the method of exhaustion, so the algorithm is easy attacked by Square. It is the cause the security of AES algorithm is reduced. So in this paper, the AES algorithm based on Dynamic chaos keys is studied from improving confusion of the key algorithm to improve the security of the AES algorithm further more.

The contents of the paper are organized as follows: At first the two-dimensional Hénon and Chebyshev chaotic map is described, then the improved AES algorithm is applied in the color image encryption, and at last the passwords are analyzed to verify their abilities to resist the password attacks effectively. These studies confirm the improved AES algorithm with higher security.

II. TWO-DIMENSIONAL CHAOTIC MAP

Chaos is a non-linear process, its structure is complex and it is difficult to analyze and predict, but it can provide the pseudo-random sequence with good randomness, correlation and complexity. It is of higher sensitivity to its initial parameters, the same chaotic system with only small differences in their initial state will produce completely different, unrelated chaotic sequences in a short period. It will be showing exponential separation state after iteration, but because the chaos has so many excellent features, and its confidential password characteristics between the existence of close links. So it is a very natural thing to develop the modern cryptography with chaotic system[3].

A. Tow-Dimensional Hénon Map

In 1976, French astronomer Hénon had been inspired from studying globular clusters and the Lorenz attractor, he proposed the following two-dimensional map:

\[
\begin{align*}
  x_{n+1} &= -ax_n^2 + by_n + 1 \\
  y_{n+1} &= x_n
\end{align*}
\]  

In the formula \(a = 1.4, b = 0.3\). The Hénon mapping strange attractor is shown in Figure 1. Took attractor to zoom in and found that the attractor has a self-similar structure[4][5].

Jacobi determinant of map (2):

\[
J = \begin{bmatrix}
  -2ax & b \\
  1 & 0
\end{bmatrix} = -b
\]  

If \(|b| < 1\), it explains that the initial iterations area will receive, that is the Iterative area will be reduced to \(|b|\) times of the original after each iteration. Next take \(a = 1.4, b = 0.3\) to illustrate how the chaos is generated, first evaluate the two fixed point of mapping (1):

\[A(0.6314,0.6314), B(-1.1314,-1.1314)\].
By calculation, the con vectors of the Jacobi matrix in fixed point $A$ is that: $\lambda_1 = -1.924, \lambda_2 = 0.156$ so fixed point $A$ is an unstable saddle point. A stable manifold and an unstable manifold near point $A$ are formed based on two eigenvectors. As shown in Figure 2.

The figure 2 shows that the points on the unstable manifold are away from the point $A$, but the points on the stable manifold tend to the point $A$ through iterative in the vicinity of the point $A$. Because the system is non-linear, stable manifold and unstable manifolds of point $A$ is distorted away in the place far away from the point $A$.

For Hénon map, if one region of initial is selected to iterate, each step of the iterative process can be regarded as the operation of the following step for the initial area, As shown in Figure 3

- Stretch and flatten the region of initial, make its area to be reduced to 0.3 times.
- Since is negative, so flip about the graphic.
- The non-linear map itself makes the graphic be bent into a curved edge quadrilateral.

It can produce a strange attractor after several times of stretching and folding. It make the stable manifold and unstable manifold of point has Infinite times intersects by sketching and folding, the intersection point is called homoclinic point, one homo-clinic point is marked only in Figure 2.

B. Chebyshev Map

Chebyshev map equation,

$$x_{n+1} = \cos(m \arccos x_n), x_n \in [-1, 1]$$

(3)
In the equation, the value $m$ is the order of Chebyshev map, when the value $m$ is greater than 2, the map has positive Lyapunov exponent and it will be into the chaotic region. It can generate infinite length and aperiodic real-valued chaotic sequences in infinite precision conditions [6]-[8].

For Chebyshev map, when the original value is changed to $1 \times 10^{-16}$, it can produce two unrelated sequences.

Figure 4 (a) shows the relationship between map equation order $k$ and initial change step $u$ to initial sensitivity. Horizontal ordinate is order $k$, vertical coordinate is the required number of iterations for the two quite separate sequences. It is defined as the initial value sensitivity. The figure shows the relationship between the value of $d$ and the value of $k$ with the different value of $u$. As we can see, with the value of $k$ increasing, the value of $d$ will reduce, but the value does not have a great impact on the value of $d$. Furthermore, when the value of $k$ is greater than 6, the value of $d$ is no longer a significant change. When the value of $u$ is greater than $1 \times 10^{-16}$, the value of $d$ is less than 30. That is, the two sequences are unrelated after 30 iterations, when the value of $u$ is changed, the value of $d$ changes is little. When the value of $u$ is less than $1 \times 10^{-16}$, it cannot produce two unrelated sequences.

Figure 4(b) shows the influence of the initial value selection on initial sensitivity, Wherein, $k=16$, $u=10^{-12}$. As we can see, the initial value selection had no significant effect on the sensitivity, it has a peak point only at the initial value of $x = 0$.

In order to improve the security of the algorithm and the key space, the one-dimensional Chebyshev map is expanded into a two-dimensional Chebyshev map which is defined as follows:

$$\begin{align*}
x_{n+1} &= \cos(m \arccos x_n) \\
y_{n+1} &= \cos(n \arccos y_n)
\end{align*}$$

(4)

The two-dimensional Chebyshev map will be a part of the dynamic key generator in the improved algorithm of AES.

III. DESIGN OF AES ALGORITHM BASED ON TWO-DIMENSIONAL HÉNON AND CHEBYSHEV MAP

The AES algorithm is a block cipher system. The size of data packet is 128 bits, an AES algorithm with key iterated after $n$ rounds is divided into three stages [9]:

- The initial round keys do addition transform, that perform a bitwise XOR on the packets of initial key and the plaintext data.
- The operating cycle $n-1$ times, on each round the data processing accord with the following four steps 1) transform S box: transmit bytes through the check s box table.2) Line shift operator: Line cyclic left shift operation.3) Confuse Columns: get a new column with a matrix multiplied each column of the group.4) Round keys plus operator: the initial key generate each round keys after it is extended, do bitwise XOR operation with the current round key and the current round packets of data.
The last transformation: A sub-three steps: 1) s box transformation. 2) line shift operator. 3) round keys plus operator. AES encryption process is shown in Figure 5.

![Figure 5. diagram of AES encryption process](image)

The encryption algorithm based on two-dimensional Hénon and Chebyshev map is a dynamic key AES encryption algorithm, the key of the design is the dynamic changes of the AES key. The keys will change after each round of encryption, thus changing the immutable key in the original algorithm, and there is no linear relationship between the key generated and the last round key, thus it is chaotic sequence as we call. In order to achieve this goal, we have to select the chaotic map, but the different chaotic mapping algorithm has the different algorithm complexity, Including the time complexity and space complexity. One-dimensional map algorithm is simple, and its operating speed is fast, but the key space is small and it has poor security. Two-dimensional chaotic system is more complicate than the one-dimensional map, the computing speed is slower than one-dimensional, but the key space is large and it has a higher security. This paper proposes the improvement for the AES algorithm through considering the key security, speed of operation and the degree of difficulty of the algorithm realized. We put the security of the key as the first premise. It can achieve smaller time and space complexity, but key space is improved, so it avoids the disadvantage of the traditional AES encryption algorithm.

According to the existing AES algorithm and chaotic map, the round keys are produced by combination of the AES algorithm and the chaotic map. The algorithm can be according to the following steps:

1. Take the initial value \((x_0, y_0)\) of two-dimensional Hénon map and two control parameters \(a, b\) as algorithm keys, and take the two-dimensional Hénon map as the Primary key map, two sets of the chaotic key stream key 1 and key 2 are produced by iterating.

2. Take the initial value \((x_0, y_0)\) of two-dimensional Chebyshev map and two control parameters \(m, n\) as the Internal private key of the algorithm, and take the two-dimensional Chebyshev map as the secondary key map, two sets of the chaotic key stream key 1 and key 2 are produced by iterating.

Four groups of key stream perform a bitwise XOR respectively to Bitwise XOR to generate two intermediate the keys key 1 and the key 2, then generate a target key by bitwise XOR operation of the intermediate keys, this is an AES key.

We can take the two-dimensional Chebyshev map as the primary key map, the two-dimensional Hénon map as the secondary key map in the algorithm.
IV. APPLICATION OF ENCRYPTION ALGORITHM AND SECURITY ANALYSIS

A. The Applications in Image Encryption

The image transmission process is shown in Figure 6:

![Diagram of image transmission process](image)

Figure 6. diagram of image transmission process

Figure 7 shows the encryption result of the application of the algorithm on a 512 × 512 digital image, figure 7(a) is the original color Lena image, figure 7(b) is the encrypted image by the key in which there is 
\(x_0, y_0 = (0.2, 0.21), \ a = 1.4, \ b = 0.3\).

![Original Lena image](image)

Figure 7. (a) the original Lena image

![Encrypted Lena image](image)

Figure 7. (b) the encrypted image

IV. APPLICATION OF ENCRYPTION ALGORITHM AND SECURITY ANALYSIS

A. The Applications in Image Encryption

The image transmission process is shown in Figure 6:

![Diagram of image transmission process](image)

Figure 6. diagram of image transmission process

Figure 7 shows the encryption result of the application of the algorithm on a 512 × 512 digital image, figure 7(a) is the original color Lena image, figure 7(b) is the encrypted image by the key in which there is 
\(x_0, y_0 = (0.2, 0.21), \ a = 1.4, \ b = 0.3\).

![Original Lena image](image)

Figure 7. (a) the original Lena image

![Encrypted Lena image](image)

Figure 7. (b) the encrypted image

B. Algorithm security analysis

1. Key space analysis:

According to the algorithm, it can provide a huge key space for the encryption algorithm by using two-dimensional chaotic map. It takes the initial value \((x_0, y_0)\) of two-dimensional Hénon chaotic map as the initial key of encryption / decryption, the selection of the initial value \((x_0, y_0)\) has Infinity from the theory, but taking the initial values \((x_0, y_0)\) of two-dimensional Chebyshev map and two control parameters \(m, n\) as the Internal private key of the algorithm, it can completely meet the safety requirements of the algorithm. Obviously, it is not realistic by using the exhaustive search method to attack for such a large key space.

2. Key sensitivity analysis:

Due to the complicated dynamic performance of two-dimensional Hénon chaotic map, the output sequence on the initial conditions is sensitive very much, the algorithm is also extremely sensitive characteristic to the key, of which slight change will result in a completely different ciphertext. We use two methods to test the sensitivity of the key.

a) Use the very close key to the encryption key to decrypt, then view the results of decryption

Figure 8 shows the test result (1) of the key sensitivity in the algorithm. Figure 8(a) is the Decrypted image by the key in which there is \((x_0, y_0) = (0.2, 0.21), \ a = 1.4, \ b = 0.3\). Figure 8(b) is the Decrypted image by the key in which there is \((x_0, y_0) = (0.200001, 0.21), \ a = 1.4, \ b = 0.3\).

![Test result of key sensitivity (1)](image)

Figure 8. the test result of key sensitivity (1)

Figure 9(a) is the encrypted image by the key in which there is \((x_0, y_0) = (0.2, 0.21), \ a = 1.4, \ b = 0.3\). Figure 9(b) is the encrypted image by the key in which there is \((x_0, y_0) = (0.2100001, 0.21), \ a = 1.4, \ b = 0.3\).

![Encrypted image after key change](image)
9(c) is the color difference image of figure 9(a) and figure 9(b). Figure 9(d) is figure 9(a) and figure 9(b) a red component color difference image, Figure 9(e) is figure 9(a) and figure 9(b) a green component color difference image, Figure 9(f) is figure 9(a) and figure 9(b) a blue component color difference image.

Figure 9. The test result of key sensitivity (2)

(3) Analysis of Statistical property:

According to Shannon’s idea, the code breakers can attack a large part of the password systems by using the methods of statistical analysis [10]-[15]. Statistical analysis is the mean that the code breakers can decipher the passwords by using the rules of plaintext, they compare the ciphertext or the difference among the ciphertexts by Statistical analysis, find out the rules of the ciphertext, then compare the plaintext or the difference among the plaintexts again, at last deduce the transformation relation between plaintext and ciphertext.

The dynamic performance of the Hénon chaotic system is extremely complex, so it results in the more complex statistical relationship between the plaintext and ciphertext. Even if the opponents get a statistical relationship between the plaintext and ciphertext, they also can’t deduce the keys. From the figure 10(a) is the histogram of the original picture, the figure 10(b) is the histogram the encrypted image. The histogram of the encrypted image distributed evenly.

Figure 10(a). Plain Image.

Figure 10(b). Cipher Image
For comparison, 1000 adjacent pixel points at the same in the position of the plain image and the cipher image are given randomly by the author. According to the following formula

\[
    r_{xy} = \frac{\text{cov}(x, y)}{\sqrt{D(x)D(y)}}
\]

Inside the formula

\[
    \text{cov}(x, y) = \frac{1}{N} \sum_{i=1}^{N} (x_i - E(x))(y_i - E(y))
\]

\[
    E(x) = \frac{1}{N} \sum_{i=1}^{N} x_i \\
    D(x) = \frac{1}{N} \sum_{i=1}^{N} (x_i - E(x))^2
\]

By calculating the correlation coefficients between the adjacent pixels on three directions (horizontal, vertical, the main diagonal direction) in the plain image, we find that the correlation between adjacent pixels is lower, the ciphertext is more secure. The results of calculation as shown in table I, the encryption algorithm disrupt the correlation between the adjacent pixels in plain image completely, the little correlation between the adjacent pixels in the cipher image, so it can be regarded as almost random distribution, with good noise property.

<table>
<thead>
<tr>
<th>direction</th>
<th>plain image</th>
<th>Cipher image</th>
</tr>
</thead>
<tbody>
<tr>
<td>horizontal</td>
<td>0.8070</td>
<td>-0.0163</td>
</tr>
<tr>
<td>vertical</td>
<td>0.8422</td>
<td>0.1820</td>
</tr>
<tr>
<td>diagonal</td>
<td>0.9779</td>
<td>0.0938</td>
</tr>
</tbody>
</table>

For a more clear understanding of the correlation between the plain image and the cipher image, Figure 11 shows the correlation between the adjacent pixels in the images encrypted before and after on the horizontal direction. Figure 11(a) shows the correlation analysis between the adjacent pixels in the plain image. Figure 11(b) shows the correlation analysis between the adjacent pixels in the cipher image. The correlation between the adjacent pixels in the images encrypted before and after is far less than the correlation of the original image in Lena, so it indicates that the algorithm has strong anti-statistical analysis.

(4) Differential analysis:

Usually the attacker will observe the change of the image in the encrypted by the small area in the image, such as only changing one pixel, because he can crack the cipher image in this way.

To test the change of the pixels in plain image influence on the cipher image, We define the two variables-- Rate of Change in Pixels(PCR) and Average of Intensity Change Rate(AICR).

There are two cipher images, respectively \(c_1\) and \(c_2\), and there is only one pixel change in the plain images corresponding them. The intensity of the pixel at the position \((i, j)\) is marked as \(C_1(i, j)\) and \(C_2(i, j)\).

\[
    PCR = \frac{1}{W \times H} \left( \sum_{\text{pixel, not equal}} \delta(C_1(i, j), C_2(i, j)) \right)
\]

**(a) Plain Image**

**(b) Cipher Image**

---

**TABLE I. THE CORRELATION COEFFICIENTS BETWEEN THE ADJACENT PIXELS IN THE PLAIN AND CIPHER IMAGE**

- Figure 11. The Analysis Between Horizontal Adjacent Pixels
\( AICR \) is defined as the follow:

\[
AICR = \frac{1}{W \times H} \sum_{1 \leq i \leq W, 1 \leq j \leq H} \left( C_i(i,j) - C_i(i,j) \right) / 255
\]  
(7)

Inside the formula, the character \( W \) is the width and the character \( H \) is the height of the image, \( \delta(x, y) \) is a function of the formula (8) defines.

\[
\delta(x, y) = \begin{cases} 
1, & (x \neq y) \\
0, & (x = y) 
\end{cases}
\]  
(8)

We tested the change of the first pixel in the plain image on the influence of the cipher image in table II, we can see the value of the \( PCR \) and \( AICR \), while the first pixel low 8 bits of the cipher image are changed differently.

| TABLE II. THE OVERALL INFLUENCE OF THE CHANGE OF THE FIRST PIXEL IN THE PLAIN IMAGE TO THE CIPHER IMAGE |
|-------------------------------------------------|-------------------|-------------------|-------------------|-------------------|-------------------|-------------------|-------------------|-------------------|
| The number of bits changed | low 1 bit | low 2 bits | low 3 bits | low 4 bits | low 5 bits | low 6 bits | low 7 bits | low 8 bits |
| The value of BC | 0.917 | 0.917 | 0.917 | 0.917 | 0.917 | 0.917 | 0.917 | 0.917 |
| The value of AIC | 0.015 | 0.0057 | 0.0047 | 0.0232 | 0.0345 | 0.0350 | 0.0577 | 0.0455 |

As the table II shows, no matter how many bits change in the first pixel low 8 bits of the plaintext, the change of the image pixels in the ciphertext are the same, but the value of the \( AICR \) monotonically increases with the increases bits in the first pixel lower 8 bits of the plaintext.

V. CONCLUSIONS

From the above-mentioned content, centrifugal extruder, a new polymer processing machine, is provided. And by the mathematical analysis and experiments, it is shown that the centrifugal force field can provide the solid-plug conveying pressure sufficiently and stably, which can prove the industrial practicability of centrifugal extruder. And the temperature distribution of solid-plug conveying phase is achieved in which the rotor speed affects the temperature of the rotor surface, as the faster the speed, the lower the temperature.

ACKNOWLEDGMENT

This work was supported by the Research of Virtual Reality Technology for Architecture Landscape Reconstruction (the team support project of Tangshan Normal University In 2016), Project number: 2016B06. The Research on fault location technology of dynamic system based on multi sensor data fusion (the scientific research project in Tangshan Province in 2015), Project number: 15130203a. The Research on dynamic fault diagnosis technology of multi sensor data fusion (the team support project of Tangshan Normal University In 2016), Project number: 2016C08.

REFERENCES


