Abstract—To enhance the reliability and effectiveness of image encryption, a perceptron neural network based on HPW chaotic system is proposed. First, this algorithm combines Henon chaotic map with PWLCM chaotic map to get the improved chaotic map. It is called the HPW map. After that, input the array obtained from image decomposition into the perceptron neural network. Finally, it is combined with the chaotic matrix to complete digital image encryption. Throughout encryption, this encryption method simultaneously inputs two points into the perceptron neural network for operation, and uses the method of diffusion and scrambling to encrypt at the same time. In addition, the plain correlation method is used to complete the image encryption. This paper tests the encryption algorithm through 6 image encryption indexes, and the outcomes demonstrate that the algorithm has good efficiency and security.

Index Terms—cryptography, image encryption, perceptron, chaos

I. INTRODUCTION

In the 21st century with the rapid development of science and technology, information security has always been a sensitive and important topic for people [1]. At the same time, it has also been the focus of the military and diplomatic departments of various countries. Particularly after the turn of the 21st century, with the ongoing enhancement of the level of science and technology, intelligent monitoring, fingerprint recognition, face recognition, and other technologies are more and more widely used in our life, and the impact on our life is also growing. This also makes people have higher requirements on the quantity and speed of information transmission. Therefore, the importance of information security is particularly prominent [2].

As the carrier of information, images appear in people's vision all the time. Therefore, images are easily invaded during transmission, resulting in the leakage of picture information [3]. Due to the large-scale use of digital images, especially if the image involves important secrets, so it must be kept confidential before transmission.

And because some of the information involves personal privacy, copyright, and other security reasons, users do not want the information to be viewed by unauthorized persons. Therefore, it is essential to ensure user information security. Image security is the main part of network security, and image security management has become one of the most important research trends [4].

We can imagine the picture is composed of countless pixels. When an image is constantly expanded by people, we can find many small squares. And these small squares together constitute people's ordinary pictures. If we regard the image as a two-dimensional matrix, then image encryption is to transform the matrix to fulfill the goals of encryption [5].

In most of the current image encryption, the cipher is generally applied to the sender and the receiver. And then combined with the key to complete the decryption [6]. The most basic operations of image encryption are confusion and diffusion. The goal of confusion is to change the original orientation of the pixel values in the matrix. Common methods include sorting, cyclic shift, and so on. Diffusion refers to a subtle change in the pixel value of the initial image. The pixel value of the entire image will significantly change as a result. The common method is XOR operation.

However, because the image has a lot of data, significant redundancy, and a high correlation of pixels. It makes the traditional encryption method inefficient and poor security, and can not meet the needs of network technology for image encryption [7]. Because of the good characteristics of chaotic mapping, including initial value sensitivity, ergodicity, short-term predictability, and long-term unpredictability, it is frequently applied to the encryption of digital images [8]. At the same time, in recent years, many scholars have combined chaos and neural network technology with image encryption. And it has achieved good encryption results.

Ameena Marshnil, an Indian scientist, has proposed an innovative image encryption method in recent years. It improves the reliability of image encryption technology, and the peak value and signal-to-noise ratio also meet the requirements.

To meet the requirements of current network technology for image encryption technology, this paper proposes a

Yilin Han, Ye Tao, Wenyu Zhang, Wenhua Cui, and Tianwei Shi
perceptron neural network image encryption algorithm based on HPW chaotic system. Compared with other traditional neural network image encryption algorithms, the neural network is used to generate a chaotic matrix for image encryption. This algorithm is to apply a neural network as an algorithm to the process of image encryption. Then it is combined with the chaotic matrix to complete image encryption.

II. INTRODUCTION TO CHAOTIC MAPS

A. Henon chaotic map

In the mid-1960s, a two-dimensional chaotic map known as the Henon map was discovered by the scientist Henon. The formula is shown in the following formula (1).

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

(1)

where \( \mu, x \) are the parameters. \( x(n) \) is in a chaotic state. when \( 3.569945627 < \mu \leq 4 \), \( 0 < x < 1 \). Among, \( a \in (0,1.4) \), \( b \in (0.2,0.314) \). Because it can be seen from formula (1) \( y_{n+1} \) and \( x_n \) a linear relationship exists between them, It is concluded that formula (1) can be transformed as shown in (2).

\[
x_{n+1} = 1 - ax_n^2 + bx_{n-1}
\]

(2)

The Henon map bifurcation diagram is shown in Fig 1.

B. Piecewise linear chaotic map (PWLCM)

A PWLCM map is also called a piecewise linear chaotic map [9]. The form of PWLCM is relatively simple and the ergodicity is very extensive, besides it can produce a better pseudo-random sequence effect. Equation (3) depicts the definition of PWLCM.

\[
x_i = f(x_{i-1}, p) = \begin{cases} 
  x_{i-1}, & 0 < x_{i-1} < p \\
  \frac{x_{i-1} - p}{0.5 - p}, & p \leq x_{i-1} < 0.5 \\
  f(1-x_{i-1}, p), & 0.5 \leq x_{i-1} < 1 
\end{cases}
\]

(3)

C. HPW chaotic map

To enhance the effect of the chaotic matrix obtained from the chaotic map. This paper proposes an improved piecewise linear mapping scheme. It is called HPW. The algorithm combines Henon chaotic map with PWLCM chaotic map to generate a multi-chaotic system (HPW). This chaotic system enhances the randomness of the obtained chaotic matrix. At the same time, the initial value sensitivity of the chaotic system is also increased compared with the previous two systems. For the chaotic system with a large number of inherent randomness, even if the initial value changes slightly, after continuous calculation the results will be very different.

Besides, the \( 16 \times 16 \) chaotic matrix \( KEY(m,n) \) is generated by the improved HPW map. If the matrix is used as the key matrix of the encryption algorithm, compared with other encryption algorithms the key space and randomness of the encryption algorithm are greatly improved, and the key matrix is confidential during transmission. The HPW mapping formula is shown in (4).

\[
x_i = f(x_{i-1}, p) = \begin{cases} 
  f(x_{i-1} + 0.5, p), & x_{i-1} \leq 0 \\
  \frac{1 - ax_{i-1}^2 + bx_{i-2}}{p}, & 0 < x_{i-1} < p \\
  \frac{1 - ax_{i-1}^2 + bx_{i-2} - p}{0.5 - p}, & p \leq x_{i-1} < 0.5 \\
  f(1-x_{i-1}, p), & 0.5 \leq x_{i-1} < 1 \\
  f(x_{i-1} - 0.5, p), & x_{i-1} \geq 1 
\end{cases}
\]

(4)

III. IMAGE ENCRYPTION AND DECRYPTION ALGORITHM

A. Image encryption and decryption algorithm

Information security is a very important research topic...
nowadays. This paper proposes a perceptron neural network image encryption algorithm based on HPW chaotic system. The overall encryption process is shown in Fig 3.

To improve the efficiency of encryption, this algorithm has been improved on the traditional perceptron neural network.

Instead of inputting only one point into the perceptron for encryption, two points are input into the perceptron neural network concurrently for encryption. In the process of encryption, not only diffusion and scrambling operations are completed concurrently, but also the plain correlation technology is applied. It can resist the attacker from the diffusion and scrambling attacks respectively. It also can prevent the chosen plain and known plain. It improves the reliability of the encryption algorithm.

The internal encryption flow chart of the perceptron neural network is shown in Fig 4.

Specifically, the following steps are taken during encryption:

Step 1: In this paper, the 16×16 chaotic matrix $KEY(m,n)$ is generated by the HPW map. The HPW map is obtained by combining the Henon map with the PWLDM map. To improve the encryption speed, $m$ and $n$ are assigned to 16 respectively. Similarly, if the image encryption level of the image needs to be improved, $m$ and $n$ can be assigned to 256 respectively, that is, the 256×256 chaos matrix used.

Step 2: The plain image is decomposed into a two-dimensional array. To facilitate the operation, this algorithm converts the two-dimensional array into a one-dimensional array $PP_k$.

Step 3: Then move the point $PP_k$ to the left by 1 to 8 bits to get $PA_i$ to $PB_i$. Similarly, move the point $PP_{k+1}$ to the right by 1 to 8 bits to get $PB_i$ to $PB_i$. It can be used as the input layer of the perceptron.

Step 4: The values of $PA_i$ to $PA_i$ are remaindered with 16. To prevent the result of 0, it is necessary to add 1 to the equation, and finally get the subscript $m$ in $KEY(m,n)$. The subscript $n$ in $KEY(m,n)$ is obtained from $PB_i$ to $PB_i$ in the same way.

Step 5: The values of $QB_i$ to $QB_i$ are $KEY(m,n)$ plus 1. At the same time, the values of $QB_i$ to $QB_i$ need to be expanded by 1000 times for integers. Similarly, the values of $QB_i$ to $QB_i$ are $KEY(m,n)$ plus 1 and then expanded by 1000 times.

Step 6: The value of QSA is obtained by adding the sum of $PA_i$ to $PA_i$ and the sum of $QB_i$ to $QB_i$. In the same way, the value of QSB is obtained by adding the sum of $PB_i$ to $PB_i$ and the sum of $QB_i$ to $QB_i$.

Step 7: When $k>10$, that is the cycle is greater than 10 times, QSA will accumulate the results obtained in the first 10 times, and QSB is the same.

Step 8: The value of QSA is exchanged with the value of QSB, so that $CC_{k+1}$ is equal to QSA and $CC_k$ is equal to QSB.

Step 9: To improve the encryption effect and without missing every point, we add a reverse operation process in the encryption algorithm. That is to say, move $CC_k$ left by 1 to 8 bits to get $PA_i$ to $PA_i$. Similarly, move $CC_{k+1}$ right by 1 to 8 bits to get $PB_i$ to $PB_i$ as the input layer of the perceptron.

Step 10: Repeat the above steps.

Step 11: Then, the obtained $CC_k$ is converted back to a two-dimensional array. Finally, get the cipher image.

Step 12: The decryption process and encryption steps of the algorithm are the same.

B. The experimental results

The experimental environment of the algorithm is as follows: the simulation experiment software part is matlab R2018b, and the operating system is Windows 10; The hardware part uses Intel i5-7300HQ 2.50GHZCPU, 4.00G running memory, and 1TB hard disk. Fig 5 shows the encryption and decryption effect of different images.

C. Safety analysis

This chapter analyzes the security of this algorithm from the following six aspects. Besides compares the algorithm with the encryption algorithm in references [10-12].

The algorithm in reference [10] applies the plain-related image encryption method of a hyperchaotic system. First, the initial key and the pure image are input into the image encryption system; Input the initial key and the pure image into the replacement algorithm; The key stream generation process is then applied to the organized image and the initial key; Next, the encryption process is then finished by feeding the prepared picture and key stream into the encryption algorithm used in the diffusion step. This produces the cipher image.

A chaotic image encryption method with a dynamic variable selection system is applied in reference [11]. This scheme proposes a digital support vector machine algorithm.
Fig. 4. Internal encryption flow chart

![Diagram of an internal encryption flow chart](image-url)
(2) Key space
The efficiency of the encryption algorithm and the ability to fend off exhaustive attacks improve with increasing key space size [13].

The key of this algorithm is \( K = \{ x_1, x_2, p, a, b \} \), \( x_1, x_2 \in (0,1) \), \( 0 < p < 0.5 \), \( a \in (0,1.4) \), \( b \in (0.2, 0.314) \), step for \( 10^{14} \). Calculations indicate that the key space of the encryption algorithm is about \( 8.4 \times 10^{68} \). It is approximately equal to \( 2^{230} \).

If the key space is larger than \( 2^{230} \), the effect of this image encryption algorithm is better. In addition, we can also use the \( KEY(m,n) \) matrix as the key matrix for the image, and pass the matrix to the message receiver. Therefore, from the perspective of key space, it can be concluded that the encryption algorithm in this paper is effective and can prevent exhaustive attacks well. The comparison of key space is shown in Table 2, it can also see that the encryption key space in this paper is larger.

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Keys space</td>
<td>( 10^{69} )</td>
<td>( 10^{69} )</td>
<td>( 10^{60} )</td>
<td>( 10^{72} )</td>
</tr>
</tbody>
</table>

(3) Key sensitivity
According to the definition of key sensitivity, the higher the key sensitivity, the better the encryption performance of the algorithm [14]. NPCR and UACI are the main values for judging key sensitivity and plain sensitivity [15].

When NPCR and UACI are closer to the ideal sum 99.6094% and 33.4635%, the encryption effect will be better. In this paper, the key is changed 100 times, and the results obtained each time are ideal. Finally, the average value is calculated. Formulas (5) and (6) are the calculation methods of NPCR and UACI.

\[
NPCR = \frac{1}{M \times N} \sum_{i=1}^{M} \sum_{j=1}^{N} D(i,j) \times 100\%
\]

\[
UACI = \frac{1}{M \times N} \sum_{i=1}^{M} \sum_{j=1}^{N} \left| C(i,j) - C(i,j) \right| \times 100\%
\]

The average values of NPCR and UACI are shown in Table 3. The algorithm is also very advantageous in key sensitivity.

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>NPCR (%)</td>
<td>99.6032</td>
<td>99.2174</td>
<td>99.6200</td>
<td>99.6100</td>
</tr>
<tr>
<td>UACI (%)</td>
<td>33.4832</td>
<td>33.2904</td>
<td>33.4800</td>
<td>33.5700</td>
</tr>
</tbody>
</table>

In addition, to verify the key sensitivity, we also change the initial value and main parameters of the key, the change value is 1, and only one parameter is changed at a time. Fig 6 shows the comparison between the changed cipher and cipher difference images.
It can also see the key sensitivity of the encryption algorithm has improved.

(4) Plain sensitivity
To changing the key, we also modified the pixel value of the plain image. It can analyze the sensitivity of plain.

In order to obtain accurate experimental results, the pixels of the plain image is randomly modified 100 times. Each time the values of NPCR and UACI are very close to the ideal values. In the end, the 100 times average values of NPCR and UACI are calculated. The plain sensitivity of this scheme is ideal. So it can effectively resist differential attacks. This better proves the security of the algorithm in this paper.

Table 4 is a comparative analysis of plain sensitivity.

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>NPCR (%)</td>
<td>99.5934</td>
<td>99.2174</td>
<td>99.6100</td>
<td>99.7200</td>
</tr>
<tr>
<td>UACI (%)</td>
<td>33.5535</td>
<td>33.4500</td>
<td>33.7400</td>
<td>33.7400</td>
</tr>
</tbody>
</table>

(5) Cipher statistical characteristics
According to the definition of cipher statistics, the weaker the correlation between nearby pixels, the better the image encryption effect [16]. Fig 7 shows the histogram of Lisa's, Girl's, and Town's plain and cipher. The peak value of the histogram of the plain image is relatively volatile. However, the peak value of the cipher image is relatively stable. Indicating that the correlation between adjacent pixels of the encrypted image is relatively small.

To better show this conclusion, this paper also calculates and shows the correlation between pixels in the horizontal, vertical, and diagonal directions of plain image and cipher image. In the operation, N pairs of adjacent pixels need to be randomly selected in the image. The gray value is \((u_i, v_j)\).

The formula between \(i = 1, 2, \ldots, N\), \(u = \{u_i\}\) and \(v = \{v_j\}\) is shown in (7).

\[
\begin{align*}
    r_{xy} & = \frac{\text{cov}(\sigma, \tau)}{\sqrt{D(\sigma)D(\tau)}} \\
    \text{cov}(\sigma, \tau) & = \frac{1}{N} \sum \left( x_i - \overline{x} \right) \left( y_j - \overline{y} \right) \\
    D(\sigma) & = \frac{1}{N} \sum (\sigma_i - \overline{\sigma})^2 \\
    E(\sigma) & = \frac{1}{N} \sum \sigma_i
\end{align*}
\] (7)
When \( u_i \) is \( (x_i, y_i) \) , \( v_i \) is \( (x_i + 1, y_i) \) , the horizontal correlation is obtained; When \( v_i \) is \( (x_i, y_i + 1) \) , get the vertical correlation; When \( v_i \) is \( (x_i + 1, y_i + 1) \) , get the diagonal correlation. The correlation coefficients of the three images in different directions are shown in Table 5. Then it compares with the algorithms in other references.

**TABLE 5**

<table>
<thead>
<tr>
<th>Algorithm</th>
<th>Horizontal</th>
<th>Vertical</th>
<th>Diagonal</th>
</tr>
</thead>
<tbody>
<tr>
<td>Proposed Lisa (plain)</td>
<td>0.9604</td>
<td>0.9610</td>
<td>0.9398</td>
</tr>
<tr>
<td>Proposed Lisa (cipher)</td>
<td>-0.0074</td>
<td>-0.0019</td>
<td>0.0210</td>
</tr>
<tr>
<td>Proposed Girl (plain)</td>
<td>0.9803</td>
<td>0.9756</td>
<td>0.9625</td>
</tr>
<tr>
<td>Proposed Girl (cipher)</td>
<td>-0.0105</td>
<td>-0.0354</td>
<td>-0.0287</td>
</tr>
<tr>
<td>Proposed Town (plain)</td>
<td>0.9476</td>
<td>0.9512</td>
<td>0.9194</td>
</tr>
<tr>
<td>Proposed Town (cipher)</td>
<td>-0.0118</td>
<td>0.0160</td>
<td>-0.0056</td>
</tr>
<tr>
<td>Ref.[13] (cipher)</td>
<td>-0.0331</td>
<td>0.0024</td>
<td>0.0041</td>
</tr>
<tr>
<td>Ref.[14] (cipher)</td>
<td>0.0109</td>
<td>-0.0070</td>
<td>-0.0086</td>
</tr>
<tr>
<td>Ref.[15] (cipher)</td>
<td>-0.0032</td>
<td>-0.0063</td>
<td>0.0086</td>
</tr>
</tbody>
</table>

According to the above table, the coefficients of the plain image are large, basically near to 1. It demonstrates the significant correlation between the pixels in the plain image. On the contrary, the encrypted image coefficients are relatively small, basically approaching 0. It can be proved the cipher statistics of the encryption algorithm is good.

To more intuitively prove the correlation between plain and cipher pixels in the encryption algorithm. This paper draws a pixel distribution map, as shown in Fig 8. The correlation of the plain image is close to a straight line, and the pixels of the cipher correlation image are more scattered.

This also well reflects how strongly adjacent pixels in the plain image are correlated with one another. The adjacent pixels of the cipher image have a weak correlation with one another, though. It also proves the security and reliability of the algorithm are good.

(6) Information entropy

According to the definition, the closer the information entropy is to 8, the greater the uncertainty of the encrypted image, the less information can be seen, and the better the encryption effect [17]. As shown in Table 6, the calculation results of Lisa, Girl, and town images, and compares with the information entropy of other references. There is a great difference between the information entropy of the plain image and the ideal value in this table, however the information entropy of the cipher image is closer to the ideal value, so it can be proved the encryption algorithm performs well.

**TABLE 6**

<table>
<thead>
<tr>
<th>Algorithm</th>
<th>Information entropy</th>
<th>Theoretical value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Proposed Lisa (plain)</td>
<td>7.5327</td>
<td>8</td>
</tr>
<tr>
<td>Proposed Lisa (cipher)</td>
<td>7.9332</td>
<td>8</td>
</tr>
<tr>
<td>Proposed Girl (plain)</td>
<td>7.7317</td>
<td>8</td>
</tr>
<tr>
<td>Proposed Girl (cipher)</td>
<td>7.9321</td>
<td>8</td>
</tr>
<tr>
<td>Proposed Town (plain)</td>
<td>7.4860</td>
<td>8</td>
</tr>
<tr>
<td>Proposed Town (cipher)</td>
<td>7.9353</td>
<td>8</td>
</tr>
<tr>
<td>Ref.[13] (cipher)</td>
<td>7.9969</td>
<td>8</td>
</tr>
<tr>
<td>Ref.[14] (cipher)</td>
<td>7.9993</td>
<td>8</td>
</tr>
<tr>
<td>Ref.[15] (cipher)</td>
<td>7.9967</td>
<td>8</td>
</tr>
</tbody>
</table>
Fig. 8. Distribution map of the correlations of the adjacent pixels (1)
IV. CONCLUSION

In this paper, a perceptron neural network image encryption algorithm based on HPW chaotic system is proposed. The algorithm combines HPW chaotic mapping with perceptron neural network to complete image encryption. During the encryption of images, the neural network is utilized as the algorithm. Then combined with chaotic matrix, image encryption is completed. The algorithm has four innovations. First, a new chaotic mapping HPW is obtained by combining Henon mapping with PWLCM mapping, which makes the chaotic matrix more random. Second, the two-dimensional matrix of the image is converted into a one-dimensional array, which is input into the perceptron neural network for encryption. This increases the speed of image encryption. Third, both diffusion and scrambling encryption techniques are applied. It can better resist the separation attack problem of diffusion and disturbance. Fourth, the plain correlation technology is used in the encryption process, which can resist the selected plain attack and the known plain attack. Finally, the security of encryption algorithm is analyzed. The outcomes of the experiments demonstrate the effectiveness of this encryption technique.

REFERENCES


