A New Symmetric Information Hiding Scheme Based on Cover Randomness*

FANG REN, MING-YU YU, HAI-YAN XIU, WEI HOU
School of Cyberspace Security
Xi’an University of Posts and Telecommunications
Xi’an, China
E-mail: renfang_81@163.com; 2540243256@qq.com; 13210145429@163.com; 1344033933@qq.com

Almost the existing information hiding schemes only aim to enhance performance of algorithm but ignore the security. This paper proposes a new symmetric key based information hiding scheme, aiming to increase the degree of disguise and the security. The scheme utilizes the randomness of the image cover itself to generate the secret key which has high randomness, so as to improve the effect of disguise of stego-objects and the security of information hiding scheme. Besides, the scheme does not need to set additional encryption key generator. In addition, this paper also proposes a new randomness test method, which can give more accurate quantitative test results and is suitable for testing the randomness of the cover. Experimental studies show that the randomness of the LSB of the covers and the stego-objects are almost the same, and the PSNR of embedding ciphertext is higher than embedding plaintext. Therefore, the scheme has high security and high degree of disguise.

Keywords: information hiding, randomness, randomness test method, security, degree of disguise, secret key

1. INTRODUCTION

Nowadays, information hiding technology has been applied more and more widely, and then there are some areas that can be discussed. According to the different purposes, the generalized information hiding technology can be divided into digital watermarking technology and steganography. The purpose of steganography is to protect the security of information with the image as the cover. This paper mainly discusses a method to improve the security of steganography.

So far, the main purpose of most steganography schemes is to improve the embedding capacity and reduce the distortion of the cover, but the secret key is rarely used, so its security is not high. In this respect, there are only some simple achievements. For example, Toby Sharp proposed the idea of using key in information hiding technology in 2001[1], so as to improve the security of steganography.

There are two main points to improve the security of steganography by using embedded ciphertext instead of plaintext. First, the encrypted information is more difficult to understand than the plaintext. The active attacker can not distinguish whether

Received Sep 28, 2021;
This paper has been accepted as a Long Paper for presentation at NaNA2021(Paper No. NaNA2021_paper_7)
the information is hidden after extracting the encrypted information, which improves the disguise degree of the stego-object. Second, the encrypted information is equivalent to the protection of plaintext, which increases the difficulty of decryption.

However, Sharp did not propose a specific scheme in his paper, and for more than ten years, there is few contribution and no big breakthrough in this field.

In 2012, Assad[2] proposed a key based information hiding scheme which uses efficient chaotic generator to get the secret key. The chaotic generator can generate chaotic key to encrypt the plaintext which is prepared to hide. It is valuable for information hiding scheme to some extent. But the main work in this paper concentrates on the chaotic generator, and the improvement of the algorithm itself is too superficial.

In 2018, Mitekin and Fedoseev[3] proposed a new security information hiding scheme which utilizes QIM(Quantization Index Modulation) method to generate a secret key to improve the security of the scheme, so the security of this scheme depends on QIM method which it chooses. This algorithm can prevent the statistical attack, but the algorithm is less robust against additive noise and it also needs additional encryption key generator.

The keys of these methods are all from outside of the cover, and an additional encryption key generator is required, which does not fully combine the cryptography technology with the information hiding scheme. In order to improve the convenience, it is necessary to develop an information hiding scheme which does not need the additional encryption key generator.

Fabien[4] in 1999 pointed out that some data of digital images have certain natural randomness, such as the low significant bit. In the second half of the 20th century, Golomb[5] proposed three standards of randomness to judge the randomness of a binary sequence, which has become an important reference for the research in this field. Since then, many randomness testing methods have been emerging. For example, the NIST(National Institute of Standards and Technology) proposed FIPS(Federal Information Processing Standard) 140 series algorithm[6].

According to the above results, based on the research of randomness, this paper improves and combines the above schemes. Firstly, this paper combines Randomness standards of Golomb with FIPS 140-2 algorithm, and proposes a simple randomness test formula for testing the randomness of cover. Besides, the formula is used to test the natural randomness of the image. Based on this test, and on the basis of Sharp's idea, the paper uses the natural randomness of the digital image to complete the full combination of information hiding and cryptography, and improve the security of information hiding.

There are two main research contents in this paper. Firstly, the randomness test, which can be used to test the randomness of the cover, the stego-object after hiding the information, and the key generated by using the method in this paper. There are two main purposes for exploring the randomness of image cover: First, to explore what kind of images are suitable as a cover. The essence of steganography to keep secret information secure lies in the perfection of stego-objects so that it is hard for attackers to find the information hidden in the image. Hence, selecting appropriate cover is important. If the cover itself is less random, then the cover will cause the attacker's suspicion. A cover that causes an attacker's suspicion is not recommended for information hiding. Second, the purpose of testing the randomness of the key is to research a more security method of the symmetric information hiding scheme.
Secondly, this paper researches the randomized disguise of secret information based on the cover randomness, and uses the idea of one-time-pad to put forward the idea of stego-object with high degree of disguise. This paper gives the steps of this idea, and gives a way to realize it. This idea combines the idea of cover randomness and one-time-pad. To ensure information confidentiality, a new type of steganography is proposed. This kind of steganography has strong compatibility and can be combined with the advanced ideas in information hiding technology to achieve better results.

The content of this paper is organized as follows: In the related work section, the basic randomness test algorithm, the stream cipher and the concept of reversible information hiding are introduced briefly. Then, the main idea of symmetric reversible information hiding scheme and the details of achievement are proposed. Meanwhile, experiments and performance analysis are shown.

The contributions of this paper are as follows: Firstly, this paper proposes a new random test method for testing randomness of image cover specially. Secondly, a new symmetric information hiding scheme which is based on cover randomness has proposed for the first time. Finally, there are many experiments to example correctness and feasibility of the method of this paper, so this method can be directly applied in the field where it is needed.

2. PRELIMINARIES

2.1 Test method of randomness

(A) Randomness standards of Golomb
Randomness standards of Golomb[5] is a very practical means to analyze the randomness of pseudo-random sequence. It includes the balance analysis, run length statistical analysis and correlation analysis of pseudo-random sequence, which can objectively judge whether a binary sequence has pseudo randomness.

a) In a period of a sequence, the difference between the number of 0 and 1 is at most 1.

b) In a period of a sequence, the number of runs with length of 1 accounts for 1/2 of the total number of runs. The number of runs with length of 2 accounts for 1/2^2 of the total number of runs. As above, the number of runs with length of i accounts for 1/2^i of the total number of runs. In the same length runs, the number of 0 runs and 1 runs occupy respectively one half.

c) The autocorrelation coefficient is binary. That is, for an integer K, as follows:

\[ N \cdot C(t) = \sum_{i=0}^{N-1} (2s_i - 1) \cdot (2s_{i+t} - 1) = \begin{cases} N, & t = 0 \\ K, & 1 \leq t \leq N - 1 \end{cases} \]  \hspace{1cm} (1)

(B) FIPS140-2 random test standard
FIPS140-2[6] is a security requirement standard for cryptographic modules issued by NIST. These standards and guidelines are published by NIST and widely adopted by government agencies as federal information processing standards (FIPS).

At present, the latest version of the standard was published on December 3, 2002, which provides the basis for cryptographic module evaluation, verification and final authentication. According to FIPS 140-2, the cryptographic module is a collection of
hardware, software, and/or firmware, which realizes the recognized security functions (including cryptographic algorithm and key generation) and is included in a certain boundary of cryptographic system. FIPS140-2 standard specifies the security requirements of cryptographic module, which is used in security system to protect sensitive data rather than unclassified information. In order to adapt to a wide range of cryptographic module applications and environments, four incremental and qualitative security levels are defined: level 1, level 2, level 3 and level 4.

This paper mainly analyses the randomness test standard in FIPS 140-2 level 4 and gives a brief introduction of this method. There are four random tests in FIPS140-2. Suppose the length of the sequence S to be detected is n. The length of S is n. The test criteria are as follows:

a) Monobit Test: Note that the number of 1 in S accounts for K of the total length. If \(48.625%<K<51.375\%\), it will pass the monobit test.

b) Poker Test: Divide S into \(n/4\) groups, each group has the same length and is four bits binary. If each group is converted to hexadecimal, S will be converted to \(n/4\) hexadecimal numbers, and the frequency of each hexadecimal number is \(f_i\), \(i=0,1,...,15\), let

\[
p = \frac{16}{n} \sum_{i=0}^{15} f_i^2 - \frac{n}{4}
\]  

If \(2.16<p<46.17\), it will pass the poker test.

c) Runs Test: If 0 runs and 1 runs meet the following table, runs test will be passed. Seeing the Table 1 for details.

<table>
<thead>
<tr>
<th>Length of Run</th>
<th>Required Interval</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>11.58%&lt;n~13.43%n</td>
</tr>
<tr>
<td>2</td>
<td>5.57%&lt;n~6.93%n</td>
</tr>
<tr>
<td>3</td>
<td>2.635%&lt;n~3.615%n</td>
</tr>
<tr>
<td>4</td>
<td>1.02%&lt;n~1.92%n</td>
</tr>
<tr>
<td>5</td>
<td>0.515%&lt;n~1.045%n</td>
</tr>
<tr>
<td>(\geq 6)</td>
<td>0.515%&lt;n~1.045%n</td>
</tr>
</tbody>
</table>

\[d)\] Long Runs Test: If the length of the longest 0 run or 1 run is less than 0.13% n, it will pass the long runs test.

2.2 Information Hiding Technology

Information hiding[7][8][9][10] is to hide the information that needs to be kept secret in some covers, but the cover itself does not change much and will not cause doubt, so as to achieve the purpose of hiding information. In short, information hiding is to hide important information in ordinary digital media.

Based on the idea of cryptography, information hiding with the secret key can improve the confidentiality[10]. The model is as Fig. 1.
2.3 Reversible information hiding technology

Reversible data hiding (RDH)[11], also known as lossless or reversible data hiding, has been fully developed and studied in the past decades. The original intention of this technology is to eliminate the cover image distortion caused by embedding secret information. In the RDH, because of embedding secret information, the cover image has a permanent distortion which is irreparable. Although in general this distortion can be ignored, in some special cases this unavoidable distortion is strictly prohibited, and the cover image must be completely restored. Based on this special situation, a new information hiding scheme is proposed which is reversible information hiding. The model is as Fig. 2.

The typical algorithms of reversible information hiding include: Difference Expansion (DE)[12][13], Prediction Error Expansion (PEE) [14][15], Histogram Shifting (HS)[16][17], Prediction Error Histogram (HS-PEE) [18][19], etc.

Because the later experiment uses histogram shifting, here is an introduction of HS:

(A) Embedding

a) Through the gray value histogram of the cover, and find the peak point \( h \) (gray value \( G_h \)) and zero-point \( l \) (gray value \( G_l \)). Then the histogram is shifted to make a gray value empty.

b) Apply reversible information hiding scheme to secret information \( Mes \). If the bit of \( Mes \) is 0, the gray value of the hidden point remains unchanged. Else the bit of \( Mes \) is
1, the gray value of the hidden point changes. Then we get the stego-object. The histogram comparison is as Fig. 3.

![Histogram comparison between cover image and stego-object](image)

**Fig. 3.** Histogram comparison between cover image and stego-object

(B) **Extracting**

a) The receiver receives the stego-object and gets the secret information from the gray value $G_h$ and $(G_h \pm 1)$.

b) Translate the $l$ point to $h$ point back to get the original cover image.

2.4 **Natural randomness of cover**

Although steganography is different from cryptography, we can learn a lot from the latter, which is more in-depth. In 1883, Kerckhoff's elaborated the first principle of cryptographic engineering[20], in which he suggested that we assume that our opponent already knows how to encrypt data, so security must only depend on choosing a key. Since then, the history of cryptography has repeatedly demonstrated the limitations of "hidden security" - assuming that the enemy knows nothing about the system being used.

In information hiding technology, this problem is seldom discussed, because information hiding hides secret information in the cover. If an attacker knows that the digital signal is a stego-object, it can be said that information hiding fails at first. Therefore, it is biased to use Kerckhoff's criterion to require information hiding. However, from the perspective of more secure information hiding schemes, if Kerckhoff's criterion is followed, a more secure information hiding algorithm can be developed. Assuming
that an attacker has a strong ability and is familiar with the information hiding algorithm, but he does not have the secret key, he cannot get the secret information, so the information hiding algorithm is more secure. If the attacker's ability is not strong, that is, he does not know the specific information hiding algorithm. Even if he suspects that these digital signals are stego-objects, a high degree of disguise can dispel his suspicions, because the designer uses the method which is encrypting the plaintext with key generated by randomness of the cover and then hiding the ciphertext. This method can increase the degree of disguise of the stego-object.

So hidden information can not be found by the opponent as far as possible, so one problem needs to be studied is the randomness of the cover, which means that the hidden information as a cover has a certain degree of randomness. Take an image as an example, the general information hiding algorithms are to hide secret information to the low significant bits of the image. For an image, the lower bits should have better randomness, which is called cover randomness. If you want to disguise the object perfectly, you should try not to destroy the randomness of the cover.

3. PROPOSED SCHEME

3.1 New randomness test method

The FIPS140-2 algorithm gives the criteria for the sequence satisfying the pseudo-random sequence. This section proposes a new randomness test method based on FIPS140-2 and Golomb standards, which can quantitatively describe randomness. This method makes the test more useful for testing cover randomness of images. Specific improvements are as follows:

a) Improve the monobit test by using the balance test: balance test refers to a binary sequence in which the number of 0 and the number of 1 are basically the same, the number of 0 is \( n_0 \), the number of 1 is \( n_1 \), so the following formula is shown below:

\[
f^a = \min \left( \frac{n_0}{n_1}, \frac{n_1}{n_0} \right)
\]

The closer \( f^a \) is to 1, the better the first test is.

b) Improve the poker test with sequence test: Sequence testing refers to the same number of 00, 01, 10, 11 in a binary sequence. The testing steps are as follows:

Step 1. Record the number of 00, 01, 10, 11 in the binary sequence as \( q_{00}, q_{01}, q_{10}, q_{11} \), and find the smallest and next smallest as \( q_{s1}, q_{s2} \). Sequence length is denoted as \( N \):

Step 2. Calculate the following formula:

\[
f^b = \frac{q_{s1} + q_{s2}}{N} \times 2
\]

The closer \( f^b \) is to 1, the better the second test is.

c) Improve the run test in FIPS140-2 by using the Golomb randomness standards. The run test in Golomb randomness standards is as follows: In a period of a sequence, the number of runs with length of 1 accounts for 1/2 of the total number of runs. The number of runs with length of 2 accounts for 1/2^2 of the total number of runs. As above, the number of runs with length of \( i \) accounts for 1/2^i of the total number of runs. In the
same length runs, the number of 0 runs and 1 runs occupy respectively one half. So, the
test steps are as follows:

Firstly, count the number of 0, 1 runs for each length, as the Table 2 shown.
Let \( N = A_i + A_i + \ldots + A_i + B_i + B_i + \ldots + B_i \).
Secondly, count the number of runs with length \( i \) as \( 1/2^i \) of the total runs:
\[
f^c_{ii} = \min \left( \frac{1}{1}, \frac{2^i}{A_i + B_i} \right)
\]

(5)

| Table 2. Run-length statistics table |
|----------------|----------------|
| Length of Run | 0 run | 1 run |
| 1             | \(A_1\) | \(B_1\) |
| 2             | \(A_2\) | \(B_2\) |
| ...           | ...   | ...   |
| max\(i\)       | \(A_{\text{max}}\) | \(B_{\text{max}}\) |

Thirdly, calculate the average value of all \( f^c_{ii} \) as \( f^c_1 \). Calculate the second half
of the runs test:
\[
f^c_{2i} = \min \left( \frac{A_i}{B_i}, \frac{B_i}{A_i} \right)
\]

(6)

Then, calculate the average value of all \( f^c_{2i} \) as \( f^c_2 \).

Finally, the average values of \( f^c_1 \) and \( f^c_2 \) are calculated as \( f \). And the closer \( f \)
is to 1, the better the third test is.

d) Improve the long-run test in FIPS140-2 by using the correlation test of the
Golomb randomness standard. The correlation test of the Golomb randomness standard
refers to the sequence \( s \) for an integer \( K \).
\[
N \cdot C(t) = \sum_{i=0}^{N-1} (2x_i - 1) \cdot (2x_{i+t} - 1) = \begin{cases} N, & t = 0 \\ K, & 1 \leq t \leq N - 1 \end{cases}
\]

(7)

The test steps are as follows:
The length of the record sequence is \( n \). First, the original sequence is cyclically
right-shifted \( i \) bits, \( i = 1, 2, \ldots, N - 1 \). Each right-shifted sequence is XOR-operated with
the original sequence to obtain \( R_i \).

Then, perform the first test for each \( R_i \) to get \( f^d_i \), and calculate the average value of
\( f^d_i \) to get the correlation test result \( f^d \). And the closer \( f^d \) is to 1, the better the fourth test
is.

Finally, take the average of the four tests to get the final test result,
\[
f = \frac{f^a + f^b + f^c + f^d}{4}
\]

(8)

The closer \( f \) is to 1, the better the randomness.
The above scheme has more flexibility than FIPS140-2, and can set a threshold
value \( \theta \) according to the actual needs. If the value is below \( \theta \), it does not pass, else, it
passes. Moreover, this scheme can compare the randomness of different binary
sequences.
In the randomness test of image, it can compare the change degree of the random
degree of the cover image with the random degree of the stego-object. This scheme can give the different value of the random degree whether it is good or bad, and make the data changed at a glance.

3.2 Achievement of proposed scheme

The word randomized disguise comes from the term of information hiding, which is called the cover embedded in secret information as the stego-object. This paper uses the natural randomness of the image to randomize secret information, and then hides the randomized information in the cover image. Due to the randomness of the cover itself, the secret information that needs to be hidden is random, so the randomness of the stego-object is not destroyed. Thus, a more perfect disguise can be made, making the attributes of the stego-object closer to the original image, making the secret information more difficult to discover, and improving the security of information hiding technology.

(A) Description of scheme

In cryptography, a secret key can be used to complete the confidentiality of information. Shannon mentioned in his paper that the most secure encryption method is one-time-pad[21], because the amount of mutual information between plain text and cipher text is 0. Then for a natural image, using the randomness of the natural image itself to hide the plain text in a cipher-like way is similar to one-time-pad.

According to the Kerckhoffs criterion[20], the security of a security protection system is not based on its algorithm, but on the key being secret to the attackers. Therefore, the security of a communication transmission depends directly on the key space, while the key space of one-time-pad is $2^n$ ($n$ is the key length), which is quite large.

In one-time-pad, the key is a true random sequence, which guarantees that the ciphertext is completely independent of the plaintext. This paper refers to this method and takes advantage of the randomness of the natural image, the key can be extracted from the image and used to encrypt plaintext, then we can get the ciphertext and hide it in the image. Because encryption uses a random key, ciphertext can be randomized so that the cover embedded in the secret information, i.e., the stego-object, also has the randomness that the original image has, which is equivalent to disguising the secret information perfectly. So, all aspects of the stego-object are close to the original image.

In the practical application of this scheme, this paper use the mind of the stream cipher. Stream cipher is a basic symmetric cryptosystem and has been one of the main cryptographic technologies used in military and diplomatic occasions.

(B) An instance of scheme

The confidentiality of one-time-pad depends on the randomness of the key. Since natural images have high randomness, they can be combined to achieve higher encryption security. In order to extract the key with high randomness, the low significant bits of grayscale image is used as the reserve key to generate the key. In order to improve the robustness of the key, this paper uses the statistical characteristics of the low significant bits of grayscale image to generate the key. This key is both random and robust, and can be used to encrypt plain text, and then hide it. So, the information hiding algorithm is highly secure.
a) Key extraction steps

Because of the randomness of the lowest bits, the lowest bits of the picture can be extracted as a preliminary key. Next, there are two processes for the preparatory key. The first is to change it into a binary sequence, then group it into groups, the number of groups is the number of bits of the key, and use the number of 0, 1 of each group to get the final key. The steps are as follows:

Step1. For a 256-level grayscale image, treated as an \( n \times n \) matrix, the reserve key can be extracted by the following formula:

\[
\begin{pmatrix}
g_{11} & \ldots & g_{1n} \\
\vdots & \ddots & \vdots \\
g_{n1} & \ldots & g_{nn}
\end{pmatrix} \mod 2 =
\begin{pmatrix}
k_{11} & \ldots & k_{1n} \\
\vdots & \ddots & \vdots \\
k_{n1} & \ldots & k_{nn}
\end{pmatrix}
\]  

(9)

Step2. Turn the prepared key into a binary sequence:

\[
\begin{pmatrix}
k_{11} & \ldots & k_{1n} \\
\vdots & \ddots & \vdots \\
k_{n1} & \ldots & k_{nn}
\end{pmatrix} \rightarrow
\begin{pmatrix}
k_{11} & k_{1n} & k_{21} & k_{2n} & \ldots & k_{nn}
\end{pmatrix}
\]  

(10)

Step3. Divide this binary sequence into \( m \) groups, \( m \) requires an odd number. Set the key sequence to \( K_i \) and the key generation formula is as follows:

\[
K_i = \begin{cases} 
0 & \text{number of 0 in group } i \geq \text{number of 1 in group } i \\
1 & \text{number of 1 in group } i > \text{number of 0 in group } i 
\end{cases}
\]  

(11)

b) Embedding step:

Step1. Extract key from the cover using the method of 3.2.(B).a).

Step2. Encrypt the plaintext with the key using the method of one-time-pad.

Step3. Use the reversible information hiding based on Histogram Shift (see 2.3) to write ciphertext into the cover and get stego-object.

The main structure of these steps is as Fig. 4.

![Fig. 4. Randomized disguise process diagram](image)

c) Extracting and decryption step

Because the reversible information hiding technique is used here, the cover can be recovered directly from the stego-object, so the steps are as follows:

Step1. The receiver receives the Stego-object, extracts the Ciphertext, and recovers the Cover.

Step2. Extract Keys from Cover using the same method as the Embedding step.

Step3. Decrypt Ciphertext with Key to get Plaintext.

The main structure of these steps is as Fig. 5.
4. EXPERIMENT

4.1 Randomness test

This section mainly compares the similarities and differences between the FIPS140-2 test and the randomness test method in this paper. The purpose of this section is to illustrate the advantages and applicability of this method in testing cover randomness compared with FIPS140-2 test through specific data.

Using Matlab to generate 20,000-bit pseudo-random sequence, using FIPS140-2 test and improved randomness test respectively, the experimental results are given.

There are specific numerical requirements for the 20,000-bit FIPS140-2 test, as described below. The length of the test sequence S is 2000, and the test criteria are as follows:

a) Monobit Test: Note that the number of 1 in S as K in the total length. If 9725<K<10275, it will pass the monobit test.

b) Poker Test: Divide S into 5000 groups, each group has the same length and is four bits binary. If each group is converted to hexadecimal, S will be converted to 5000 hexadecimal numbers, and the frequency of each hexadecimal number is $f_i, i = 0, 1, ..., 15$, let

$$p = \frac{16}{5000} \sum_{i=0}^{15} f_i^2 - 5000$$ (12)

If 2.16<$p$<46.17, it will pass the poker test.

c) Runs Test: If 0 runs and 1 runs meet the following table, the runs test will be passed. The table is shown below:

<table>
<thead>
<tr>
<th>Length of Run</th>
<th>Required Interval</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>2315~2685</td>
</tr>
<tr>
<td>2</td>
<td>1114~1386</td>
</tr>
<tr>
<td>3</td>
<td>527~723</td>
</tr>
<tr>
<td>4</td>
<td>240~384</td>
</tr>
<tr>
<td>5</td>
<td>103~209</td>
</tr>
<tr>
<td>≥ 6</td>
<td>103~209</td>
</tr>
</tbody>
</table>
Long Runs Test: If the length of the longest 0 run or 1 run is less than 26, it will pass the long runs test.

This experiment was repeated five times and the results are as Table 4.

By comparison, it can be found that the original algorithm only has a qualitative description, the discriminant method is rough, and the improved algorithm is more conducive to the comparative test. The relative strength of randomness can be compared by numerical values. Using the pseudo-random sequences passed by FIPS140-2 test, these pseudo-random sequences are tested with the algorithm of this paper, and the results are all above 0.9.

Table 4. Test method comparison table

<table>
<thead>
<tr>
<th>Test Number</th>
<th>Test Project Number</th>
<th>FIPS140-2</th>
<th>Algorithm of This Paper</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1</td>
<td>Pass</td>
<td>0.9929</td>
</tr>
<tr>
<td></td>
<td>2</td>
<td>Pass</td>
<td>0.9848</td>
</tr>
<tr>
<td></td>
<td>3</td>
<td>Pass</td>
<td>0.9633</td>
</tr>
<tr>
<td></td>
<td>4</td>
<td>Pass</td>
<td>0.9837</td>
</tr>
<tr>
<td>Average</td>
<td>Pass</td>
<td></td>
<td>0.9812</td>
</tr>
<tr>
<td>2</td>
<td>1</td>
<td>Pass</td>
<td>0.9929</td>
</tr>
<tr>
<td></td>
<td>2</td>
<td>Pass</td>
<td>0.9848</td>
</tr>
<tr>
<td></td>
<td>3</td>
<td>Pass</td>
<td>0.9634</td>
</tr>
<tr>
<td></td>
<td>4</td>
<td>Pass</td>
<td>0.9886</td>
</tr>
<tr>
<td>Average</td>
<td>Pass</td>
<td></td>
<td>0.9824</td>
</tr>
<tr>
<td>3</td>
<td>1</td>
<td>Pass</td>
<td>0.9978</td>
</tr>
<tr>
<td></td>
<td>2</td>
<td>Pass</td>
<td>0.9953</td>
</tr>
<tr>
<td></td>
<td>3</td>
<td>Pass</td>
<td>0.9521</td>
</tr>
<tr>
<td></td>
<td>4</td>
<td>Pass</td>
<td>0.9889</td>
</tr>
<tr>
<td>Average</td>
<td>Pass</td>
<td></td>
<td>0.9835</td>
</tr>
<tr>
<td>4</td>
<td>1</td>
<td>Pass</td>
<td>0.9891</td>
</tr>
<tr>
<td></td>
<td>2</td>
<td>Pass</td>
<td>0.9890</td>
</tr>
<tr>
<td></td>
<td>3</td>
<td>Pass</td>
<td>0.9244</td>
</tr>
<tr>
<td></td>
<td>4</td>
<td>Pass</td>
<td>0.9887</td>
</tr>
<tr>
<td>Average</td>
<td>Pass</td>
<td></td>
<td>0.9728</td>
</tr>
<tr>
<td>5</td>
<td>1</td>
<td>Pass</td>
<td>0.9914</td>
</tr>
<tr>
<td></td>
<td>2</td>
<td>Pass</td>
<td>0.9914</td>
</tr>
<tr>
<td></td>
<td>3</td>
<td>Pass</td>
<td>0.9484</td>
</tr>
<tr>
<td></td>
<td>4</td>
<td>Pass</td>
<td>0.9887</td>
</tr>
<tr>
<td>Average</td>
<td>Pass</td>
<td></td>
<td>0.9799</td>
</tr>
</tbody>
</table>

4.2 Cover natural randomness test

Using the previously improved randomness test algorithm, the following pictures are tested for the lowest bit surface randomness. The following images are the cover images, which are the original images with no hidden information. The images are as follows.
A NEW SYMMETRIC INFORMATION HIDING SCHEME BASED ON COVER RANDOMNESS

Fig. 6. Cover image

Fig. 7. The low significant bits of cover image

The following table gives the comparison between the randomness of the lowest significant bits of the images and the randomness of the key:

<table>
<thead>
<tr>
<th>Name of Image</th>
<th>Randomness of The LSB of The Covers</th>
<th>Randomness of The Key</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>m=11</td>
</tr>
<tr>
<td>lena</td>
<td>0.9836</td>
<td>0.9480</td>
</tr>
<tr>
<td>house</td>
<td>0.9883</td>
<td>0.9267</td>
</tr>
<tr>
<td>cameraman</td>
<td>0.9834</td>
<td>0.8844</td>
</tr>
<tr>
<td>goldhill</td>
<td>0.9869</td>
<td>0.9333</td>
</tr>
<tr>
<td>baboon</td>
<td>0.9784</td>
<td>0.9380</td>
</tr>
<tr>
<td>peppers</td>
<td>0.9860</td>
<td>0.9450</td>
</tr>
<tr>
<td>elaine</td>
<td>0.9813</td>
<td>0.9227</td>
</tr>
<tr>
<td>boats</td>
<td>0.9867</td>
<td>0.9408</td>
</tr>
<tr>
<td><strong>Average</strong></td>
<td><strong>0.9843</strong></td>
<td><strong>0.9299</strong></td>
</tr>
</tbody>
</table>

The key randomness extracted by the method in section 3 is lower than that of the cover. It can be seen that although the randomness of key is reduced, it still has randomness. If the randomness of the key is high, the secret key can be directly used only with the low significant bits of the cover.

Following is the embedding of plaintext into the cover using the method in III. The stego-objects and their LSB are as Fig. 8 and Fig. 9:
To sum up, the experiment shows that the change of the degree of randomness of the stego-object is not very big with the use of randomization disguise. Except for the house image, the other changes of the degree of randomness are less than 1%, so the degree of disguise is high.

Then, taking some topic images to compare the randomness of the LSB of LSB Algorithm, HS Algorithm and the Scheme of this paper. The results are as Table 7.

As we can see that randomness of LSB of our scheme is better. Therefore, the scheme of this paper can improve the randomness of LSB in topic images.

Table 6. Random test table

<table>
<thead>
<tr>
<th>Name of Image</th>
<th>Randomness of The LSB of The Covers</th>
<th>Randomness of The LSB of The stego-objects</th>
<th>Percentage of Random Difference</th>
</tr>
</thead>
<tbody>
<tr>
<td>lena</td>
<td>0.9836</td>
<td>0.9828</td>
<td>0.08%</td>
</tr>
<tr>
<td>house</td>
<td>0.9883</td>
<td>0.9309</td>
<td>5.74%</td>
</tr>
<tr>
<td>cameraman</td>
<td>0.9834</td>
<td>0.9759</td>
<td>0.75%</td>
</tr>
<tr>
<td>goldhill</td>
<td>0.9869</td>
<td>0.9855</td>
<td>0.14%</td>
</tr>
<tr>
<td>baboon</td>
<td>0.9784</td>
<td>0.9794</td>
<td>0.10%</td>
</tr>
<tr>
<td>peppers</td>
<td>0.9860</td>
<td>0.9780</td>
<td>0.80%</td>
</tr>
<tr>
<td>elaine</td>
<td>0.9813</td>
<td>0.9860</td>
<td>0.47%</td>
</tr>
<tr>
<td>boats</td>
<td>0.9867</td>
<td>0.9786</td>
<td>0.81%</td>
</tr>
<tr>
<td><strong>Average</strong></td>
<td><strong>0.9843</strong></td>
<td><strong>0.9746</strong></td>
<td><strong>0.97%</strong></td>
</tr>
</tbody>
</table>

Table 7. Randomness comparison of LSB

To sum up, the experiment shows that the change of the degree of randomness of the stego-object is not very big with the use of randomization disguise. Except for the house image, the other changes of the degree of randomness are less than 1%, so the degree of disguise is high.

Then, taking some topic images to compare the randomness of the LSB of LSB Algorithm, HS Algorithm and the Scheme of this paper. The results are as Table 7.

As we can see that randomness of LSB of our scheme is better. Therefore, the scheme of this paper can improve the randomness of LSB in topic images.
4.3 Comparison of PSNR

For the disguising effect of this method, this paper gives the following comparison table. The following figure shows the PSNR of encrypted plaintext compared with the PSNR of original plaintext to compare the disguising effect of plaintext storage. Written in plain text here is selected from Wu Chengen's 《Journey To The West》, where the percentage of messages refers to the percentage of messages in the maximum hidden capacity. The table is shown below:

<table>
<thead>
<tr>
<th>Name of Image</th>
<th>LSB Algorithm</th>
<th>HS Algorithm</th>
<th>Our Scheme</th>
</tr>
</thead>
<tbody>
<tr>
<td>cameraman</td>
<td>0.8889</td>
<td>0.9637</td>
<td>0.9759</td>
</tr>
<tr>
<td>baboon</td>
<td>0.8801</td>
<td>0.9850</td>
<td>0.9794</td>
</tr>
<tr>
<td>peppers</td>
<td>0.8810</td>
<td>0.9774</td>
<td>0.9780</td>
</tr>
<tr>
<td>elaine</td>
<td>0.8743</td>
<td>0.9860</td>
<td>0.9860</td>
</tr>
<tr>
<td><strong>Average</strong></td>
<td><strong>0.8810</strong></td>
<td><strong>0.9780</strong></td>
<td><strong>0.9798</strong></td>
</tr>
</tbody>
</table>

As can be seen from the table above, the embedded PSNR of the ciphertext encrypted by the encryption method in this paper is higher than that of the plain text. Then, a detailed comparison is made between the two figures. Seeing Fig. 10 for details.

Compared with ordinary reversible information hiding, this algorithm uses a key, which increases the security of secret information. The key is random, and according to the natural randomness of the lowest bit surface of the cover, the scheme used in this algorithm is more secure.
5. ANALYSIS OF ROBUSTNESS

Due to the LSB will change after the image is attacked, it is necessary to analyze the robustness of key generation in this paper to resist the attack. The method of generating keys in section 3.2 has certain robustness. This section improves this method to further enhance its robustness.

5.1 New robust key generation scheme

In order to improve the robustness of the generated key, this paper draws lessons from the value taking method in HS-PEE. Through experiments, the following key taking methods are obtained:

![PSNR change line chart of peppers and cameram](image)

Fig. 10. PSNR change line chart of peppers and cameram
Step1. Extract the LSB of the cover.
Step2. Divide the LSB into multiple blocks, every block as shown in Fig. 11.

\[
\begin{array}{ccc}
A_{11} & A_{12} & A_{13} \\
A_{21} & A_{22} & A_{23} \\
A_{31} & A_{32} & A_{33}
\end{array}
\]

Fig. 11. LSB block diagram

Step3. Add each element in each $3 \times 3$ block, that is, $f_i = A_{11} + A_{12} + \ldots + A_{33}$, so that $n$ $f_i$ values can be obtained.
Step4. Take the average value of $n$ $f_i$ and record it as $f_{ave}$.
Step5. Note that the key is $K$, and the formula for generating the key is as follows:

\[
K = \begin{cases} 
0 & f_i < f_{ave} \\
1 & f_i > f_{ave}
\end{cases} 
\] (13)

5.2 Experiment

This experiment modifies the LSB of the stego-object. In this section, two key extraction methods are experimented. For the first method, this section takes $m=15$. Generate 4900 bit key, change $n$ bit LSB, and the key retention rate of different methods are as follows.

<table>
<thead>
<tr>
<th>n(bit)</th>
<th>Key Retention Rate On Directly Hiding</th>
<th>Key Retention Rate On Method Of This Paper</th>
<th>Key Retention Rate On Method Of New Method</th>
</tr>
</thead>
<tbody>
<tr>
<td>441</td>
<td>91%</td>
<td>96.76%</td>
<td>97.55%</td>
</tr>
<tr>
<td>882</td>
<td>82%</td>
<td>94.36%</td>
<td>95.76%</td>
</tr>
<tr>
<td>1323</td>
<td>73%</td>
<td>91.04%</td>
<td>94.12%</td>
</tr>
<tr>
<td>1764</td>
<td>64%</td>
<td>90.27%</td>
<td>92.20%</td>
</tr>
<tr>
<td>2205</td>
<td>55%</td>
<td>87.70%</td>
<td>90.70%</td>
</tr>
<tr>
<td>2646</td>
<td>46%</td>
<td>85.91%</td>
<td>88.43%</td>
</tr>
<tr>
<td>3087</td>
<td>37%</td>
<td>84.83%</td>
<td>87.73%</td>
</tr>
<tr>
<td>3528</td>
<td>28%</td>
<td>83.59%</td>
<td>85.53%</td>
</tr>
<tr>
<td>3969</td>
<td>19%</td>
<td>81.98%</td>
<td>84.80%</td>
</tr>
<tr>
<td>4410</td>
<td>10%</td>
<td>80.07%</td>
<td>83.10%</td>
</tr>
</tbody>
</table>

The experiment here indicates that when the number of modified bit reaches 2205 bit, the new method still has about 90% key retention rate. And when the changed bit reaches 4410 bit, the new method has 8.3 times the key retention rate compared with the directly hiding. It can be seen that the new method really improves the robustness.

6. CONCLUSIONS
In order to increase the degree of disguise, and the security of information hiding scheme. A new symmetric information hiding scheme is proposed. This scheme is based on cover randomness to encrypt the plaintext which needs be hidden. Because of the cover randomness, the process of encryption is similar to the idea of one-time-pad. The innovation of this paper not only makes use of the randomness of cover, but also utilizes the attribution of RDH to select key from the cover. Thus, the scheme proposed in this paper does not need the addition key generation when the encryption operation is executed in the information hiding scheme. More than this, this paper proposes a new quantitative randomness test method which is suitable for testing the randomness of cover. Therefore, the new randomness test method can assist the experiment of the new information hiding scheme in this paper. Experimental results show that the new randomness test method does be suitable for testing the randomness of cover and the new information hiding scheme can increase the effect of disguise and the security.

ACKNOWLEDGMENT

This paper was supported by the National Nature Science Foundation of China (Program No.61902315, 61802243), the Natural Science Basic Research Plan of Shaanxi Province of China (Program No. 2021JM-463), and the Graduate Innovation Fund of Xi’an University of Posts and Telecommunications (CXJLY202039).

REFERENCES

10. C. P. Sunath, T. Santanam, G. Umamaheswari. “A study of various steganographic techniques used for information hiding”. International Journal of
A NEW SYMMETRIC INFORMATION HIDING SCHEME BASED ON COVER RANDOMNESS


Fang Ren (任方) received his PhD degree in cryptography from Xidian University in 2012. Now he is an associate professor of Xi’an University of Posts and Telecommunications. His research interests include information security, digital image watermark and code based cryptography.

Mingyu Yu (于明宇) is currently pursuing the Master’s degree in cyberspace security from Xi’an university of Posts and communications, Shanxi. His research interests information hiding, cover randomness and cryptography.
Haiyan Xiu (修海燕) received her B.S. degree in Information Security from Xi’an University of Posts and Telecommunications. Her research interests include post-quantum cryptography and information hiding.

Wei Hou (侯伟) is currently pursuing the Master’s degree in information security from Xi’an university of Posts and communications, Shannxi. His research interests information hiding and reversible data hiding.