JOURNAL OF INFORMATION SCIENCE AND ENGINEERING 39, 149-166 (2023)
DOI: 10.6688/JISE.202301_39(1).0009

A New Symmetric Information Hiding Scheme Based on Cover Randomness

FANG REN, MING-YU YU+, HAI-YAN XIU AND WEI HOU
School of Cyberspace Security
Xi'an University of Posts and Telecommunications
Xi'an, 710121 P.R. China
E-mail: renfang_81@163.com; 2540243256@qq.com+;
13210145429@163.com; 1344033933@qq.com

This paper proposes a new symmetric information hiding scheme, aiming to increase the degree of disguise and the security. This 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. 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 new information hiding method can improve the degree of disguise of the stego-object and the security of the steganographic algorithm, and enhance the robustness of the information hiding to some extent.

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 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 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.

For more than ten years, the methods of using a secret key for information hiding basically follow the idea of Toby Sharp, and there is no big breakthrough. The keys of

Received September 28, 2019; revised November 4, 2021; accepted December 13, 2021.
Communicated by Xiaohong Jiang.
+ Corresponding author.

these methods are all from outside of the cover, and an additional encryption key is required, which does not fully combine the cryptography technology with the information hiding scheme.

Fabien [2] 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 [3] 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 proposed FISD 140 series algorithm [4].

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 FISD 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: The first purpose is to explore what kinds 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. So, selecting appropriate cover is important. If the cover is less random, then it will cause the attacker's suspicion. A cover that causes an attacker's suspicion is not recommended for information hiding. The second purpose 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 [3] 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:

$$N \cdot C(t) = \sum_{i=0}^{N-1} (2s_i - 1) \cdot (2s_{i+1} - 1) = \begin{cases} N, t = 0 \\ K, 1 \le t \le N-1 \end{cases}. \quad (1)$$

(B) FIPS140-2 random test standard

FIPS140-2 [4] 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

$$p = \frac{16}{\frac{n}{4}} \sum_{i=0}^{15} f_i^2 - \frac{n}{4}. \tag{2}$$

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

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

Table 1. Run test pass table.

Length of Run	Required Interval
1	11.58%*n*~13.43%*n*
2	5.57%*n*~6.93%*n*
3	2.635%*n*~3.615%*n*
4	1.02%*n*~1.92%*n*
5	0.515%*n*~1.045%*n*
≥6	0.515%*n*~1.045%*n*

(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 [5-8] 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 [8]. The model is as Fig. 1.

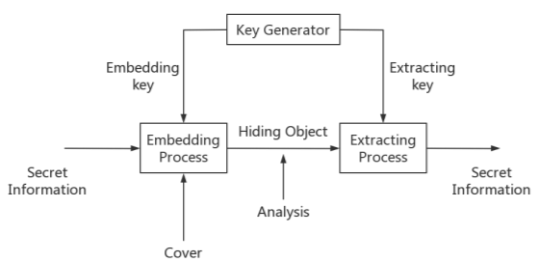


Fig. 1. General model of key based information hiding.

2.3 Reversible Information Hiding Technology

Reversible data hiding (RDH) [9], 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

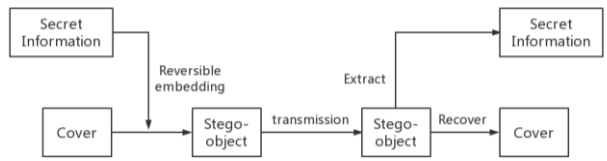


Fig. 2. Communication model of reversible information hiding.

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) [10, 11], Prediction Error Expansion (PEE) [12, 13], Histogram Shifting (HS) [14, 15], Prediction Error Histogram (HS-PEE) [16, 17], *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.

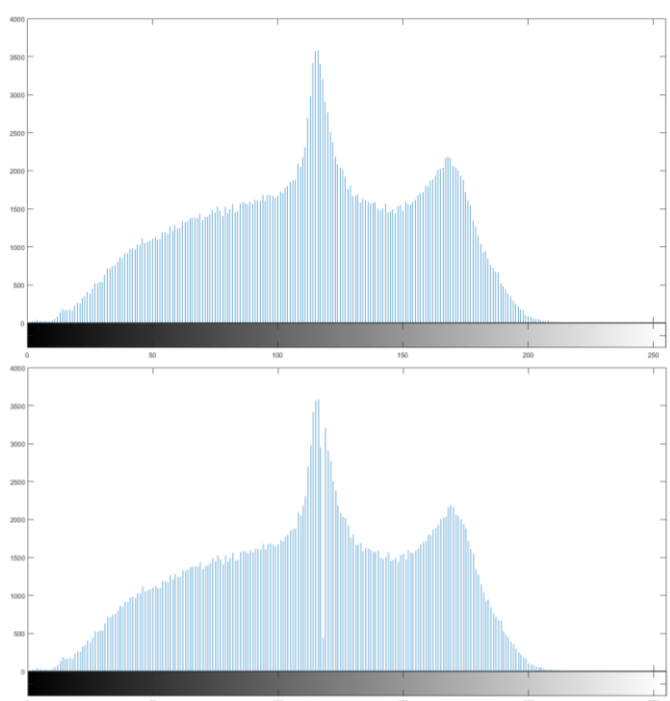


Fig. 3. Histogram comparison between cover image and stego-object.

(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, Kerckhoffs elaborated the first principle of cryptographic engineering [18], 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 Kerckhoffs criterion to require information hiding. However, from the perspective of more secure information hiding schemes, if Kerckhoffs 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 num-

ber of 0 is n_0, the number of 1 is n_1, so the following formula is shown below:

$$f^a = \min(\frac{n_0}{n_1}, \frac{n_1}{n_0}). \tag{3}$$

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:

$$f^b = \frac{q_{s1} + q_{s2}}{N} \times 2. \tag{4}$$

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

(e) 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 account 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 run and 1 run occupy respectively one half. So, the test steps are as follows:

Firstly, count the number of 0, 1 runs for each length, as shown in Table 2.
Let $N = A_1 + A_2 + \ldots + A_i + B_1 + B_2 + \ldots + B_i$.
Secondly, count the number of runs with length i as $1/2^i$ of the total runs:

$$f_{1i}^c = \min(\frac{\frac{A_i + B_i}{N}}{\frac{1}{2^i}}, \frac{\frac{1}{2^i}}{\frac{A_i + B_i}{N}}). \tag{5}$$

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_{maxi}	B_{maxi}

Thirdly, calculate the average value of all f_{1i}^c as f_1^c. Calculate the second half of the runs test:

$$f_{2i}^c = \min(\frac{A_i}{B_i}, \frac{B_i}{A_i}). \tag{6}$$

Then, calculate the average value of all f_{2i}^c as f_2^c.

Finally, the average values of f_1^c and f_2^c are calculated as f^c. And the closer f^c 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.

$$N \cdot C(t) = \sum_{i=0}^{N-1} (2s_i - 1) \cdot (2s_{i+1} - 1) = \begin{cases} N, t = 0 \\ K, 1 \le t \le N-1 \end{cases} \tag{7}$$

The test steps are as follows.

The length of the record sequence is n. First, the original sequence is cyclically right-shifted i bits, $i = 1, 2, ..., N-1$. 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_i^d, and calculate the average value of f_i^d 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,

$$f = \frac{f^a + f^b + f^c + f^d}{4}. \tag{8}$$

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 θ according to the actual needs. If the value is below θ, 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 [19], 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 [18], 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, and 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 uses 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 are 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:

Step 1: For a 256-level grayscale image, treated as an $n \times n$ matrix, the reserve key can be extracted by the following formula:

$$\begin{pmatrix} g_{11} & \cdots & g_{1n} \\ \cdots & \cdots & \cdots \\ g_{n1} & \cdots & g_{nn} \end{pmatrix} \bmod 2 = \begin{pmatrix} k_{11} & \cdots & k_{1n} \\ \cdots & \cdots & \cdots \\ k_{n1} & \cdots & k_{nn} \end{pmatrix}. \tag{9}$$

Step 2: Turn the prepared key into a binary sequence:

$$\begin{pmatrix} k_{11} & \cdots & k_{1n} \\ \cdots & \cdots & \cdots \\ k_{n1} & \cdots & k_{nn} \end{pmatrix} \to \left(k_{11} \quad \cdots \quad k_{1n} \quad k_{21} \quad \cdots \quad k_{2n} \quad \cdots \quad \cdots \quad k_{nn} \right). \tag{10}$$

Step 3: 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:

$$K_i = \begin{cases} 0 & \text{number of 0 in group } i > \text{number of 1 in group } i \\ 1 & \text{number of 1 in group } i > \text{number of 0 in group } i \end{cases}. \tag{11}$$

(b) *Embedding step*

Step 1: Extract key from the cover using the method of 3.2 (B.a).

Step 2: Encrypt the plaintext with the key using the method of one-time-pad.

Step 3: 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.

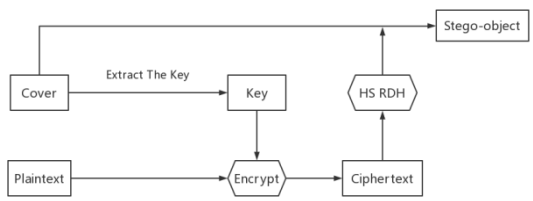


Fig. 4. Randomized disguise process diagram.

(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:

Step 1: The receiver receives the stego-object, extracts the Ciphertext, and recovers the Cover.

Step 2: Extract Keys from Cover using the same method as the Embedding step.

Step 3: Decrypt Ciphertext with Key to get Plaintext.

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

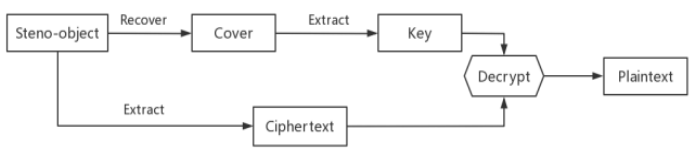


Fig. 5. Randomized disguise extracting flow.

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

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

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

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

Table 3. Run test pass table.

Length of Run	Required Interval
1	2315~2685
2	1114~1386
3	527~723
4	240~384
5	103~209
≥ 6	103~209

(d) *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.

Table 4. Test method comparison table.

Test Number	Test Project Number	FIPS140-2	Algorithm of This Paper
1	1	Pass	0.9929
	2	Pass	0.9848
	3	Pass	0.9633
	4	Pass	0.9837
	Average	**Pass**	**0.9812**
2	1	Pass	0.9929
	2	Pass	0.9848
	3	Pass	0.9634
	4	Pass	0.9886
	Average	**Pass**	**0.9824**
3	1	Pass	0.9978
	2	Pass	0.9953
	3	Pass	0.9521
	4	Pass	0.9889
	Average	**Pass**	**0.9835**
4	1	Pass	0.9891
	2	Pass	0.9890
	3	Pass	0.9244
	4	Pass	0.9887
	Average	**Pass**	**0.9728**
5	1	Pass	0.9914
	2	Pass	0.9914
	3	Pass	0.9484
	4	Pass	0.9887
	Average	**Pass**	**0.9799**

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.

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.

Fig. 6. Cover image.

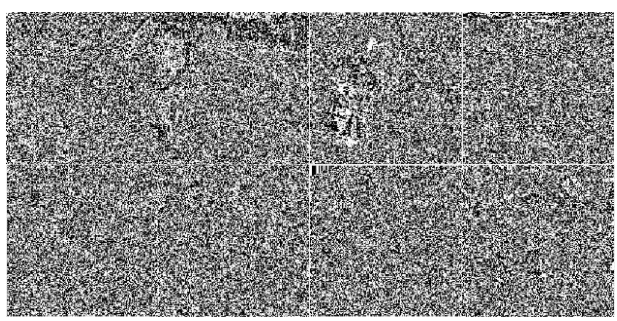


Fig. 7. The low significant bits of cover image.

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

Table 5. Randomness comparison table of low significant bits (LSB) of image and key.

Name of Image	Randomness of the LSB of the Covers	Randomness of the Key		
		$m = 11$	$m = 13$	$m = 15$
lena	0.9836	0.9480	0.9120	0.9331
house	0.9883	0.9267	0.9096	0.9071
cameraman	0.9834	0.8844	0.9491	0.9041
goldhill	0.9869	0.9333	0.9195	0.9443
baboon	0.9784	0.9380	0.9232	0.9107
peppers	0.9860	0.9450	0.9290	0.9244
elaine	0.9813	0.9227	0.9421	0.9143
boats	0.9867	0.9408	0.9294	0.9445
Average	**0.9843**	**0.9299**	**0.9267**	**0.9228**

The key randomness extracted by the method in **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 Figs. 8 and 9:

Fig. 8. Stego-objects.

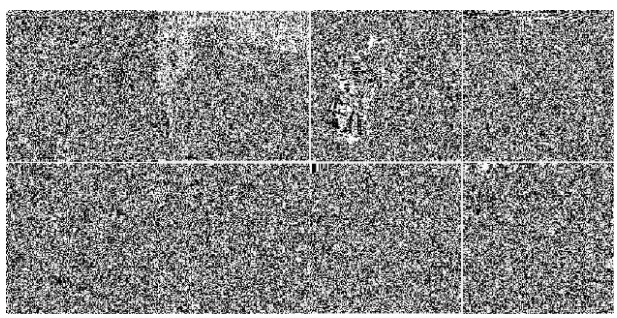


Fig. 9. The low significant bits of stego-objects.

Table 6. Random test table.

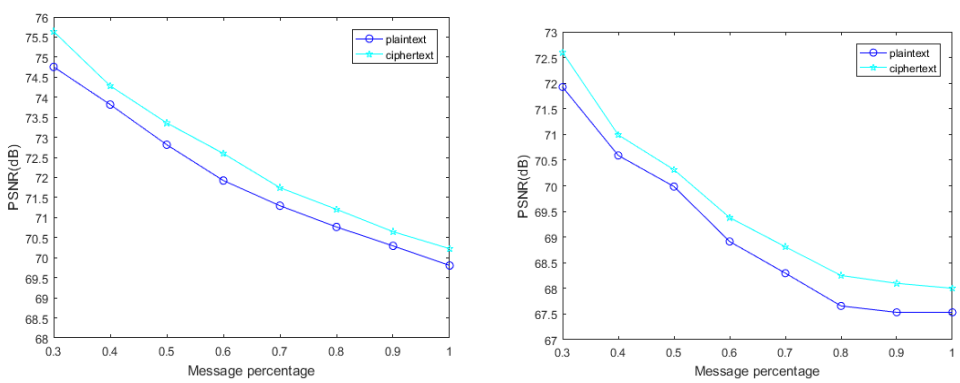
Name of Image	Randomness of the LSB of the Covers	Randomness of the LSB of the stego-objects	Percentage of Random Difference
lena	0.9836	0.9828	0.08%
house	0.9883	0.9309	5.74%
cameraman	0.9834	0.9759	0.75%
goldhill	0.9869	0.9855	0.14%
baboon	0.9784	0.9794	0.10%
peppers	0.9860	0.9780	0.80%
elaine	0.9813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

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.

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 7. Embedding rate and its PSNR table.

Name of Image	PSNR	Embedding Rate			
		25%	50%	75%	100%
lena	PSNR(Plaintext)	58.5968	58.4753	58.3627	58.2152
	PSNR(Ciphertext)	58.6138	58.4859	58.3765	58.2777
house	PSNR(Plaintext)	48.9449	48.8999	48.8532	48.8053
	PSNR(Ciphertext)	48.9517	48.9095	48.8712	48.8279
cameraman	PSNR(Plaintext)	73.1476	69.9849	68.1199	67.5333
	PSNR(Ciphertext)	73.1477	70.3132	68.4460	68.0024
goldhill	PSNR(Plaintext)	49.8991	49.8892	49.8789	49.8752
	PSNR(Ciphertext)	49.8993	49.8899	49.8834	49.8796
baboon	PSNR(Plaintext)	50.8584	50.8391	50.8213	50.8098
	PSNR(Ciphertext)	50.8597	50.8477	50.8321	50.8216
peppers	PSNR(Plaintext)	75.7629	72.8160	69.8057	69.8057
	PSNR(Ciphertext)	76.2275	73.3596	71.3411	70.2244
elaine	PSNR(Plaintext)	51.3419	51.3294	51.3149	51.3089
	PSNR(Ciphertext)	51.3429	51.3302	51.3188	51.3139
boats	PSNR(Plaintext)	50.5513	50.5250	50.5021	50.4763
	PSNR(Ciphertext)	50.5532	50.5320	50.5122	50.4939



(a) Peppers (b) Cameraman

Fig. 10. PSNR change line chart of peppers and cameramen.

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:

Step 1: Extract the LSB of the cover.
Step 2: Divide the LSB into multiple blocks, every block as shown in Fig. 11.

A_{11}	A_{12}	A_{13}
A_{21}	A_{22}	A_{23}
A_{31}	A_{31}	A_{33}

Fig. 11. LSB block diagram.

Step 3: Add each element in each 3×3 block, that is, $f_i = A_{11} + A_{12} + ... + A_{33}$, so that *n fi* values can be obtained.
Step 4: Take the average value of *n fi* and record it as f_{ave}.
Step 5: Note that the key is *K*, and the formula for generating the key is as follows:

$$K = \begin{cases} 0 & f_i < f_{ave} \\ 1 & f_i > f_{ave} \end{cases}. \tag{13}$$

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.

The experiment here indicates that when the number of modified bits reaches 2205 bits, the new method still has about 90% key retention rate. And when the changed bit reaches 4410 bits, 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.

Table 8. Key retention RATE after attack test.

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

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 (CXJJLY202039).

REFERENCES

1. T. Sharp, "An implementation of key-based digital signal steganography," in *Proceedings of International Workshop on Information Hiding*, 2001, pp. 13-26.
2. F. A. Petitcolas, R. J. Anderson, and M. G. Kuhn, "Information hiding – a survey," in *Proceedings of the IEEE*, Vol. 87, 1999, pp. 1062-1078.
3. J. Fan, X. Zhang, and H. Hou, *New Addition of Cryptography [M]*, Xidian University Press, China, 2018.

4. K. H. Brown, "Security requirements for cryptographic modules," *Federal Information Processing Standards Publication*, 1994, pp. 1-53.
5. K. Cabaj, L. Caviglione, W. Mazurczyk, *et al.*, "The new threats of information hiding: The road ahead," *IT Professional*, 2018, Vol. 20, pp. 31-39.
6. W. Mazurczyk and S. Wendzel, "Information hiding: challenges for forensic experts," *Communications of the ACM*, Vol. 61, 2017, pp. 86-94.
7. E. T. Sivadasan, "A survey paper on various reversible data hiding techniques in encrypted images" in *Proceedings of IEEE International Advance Computing Conference*, 2015, pp. 1139-1143.
8. C. P. Sumathi, T. Santanam, and G. Umamaheswari, "A study of various stegano-graphic techniques used for information hiding," *International Journal of Computer Science & Engineering Survey*, Vol. 4, 2013, pp. 9-25.
9. Y. Shi and X. Li, "Reversible data hiding: advances in the past two decades," *IEEE Access*, Vol. 4, 2016, pp. 3210-3237.
10. J. Tian, "Wavelet-based reversible watermarking for authentication," in *Proceedings of SPIE*, Vol. 4675, 2002, pp. 679-690.
11. J. Tian, "Reversible data embedding using a difference expansion," *IEEE Transactions on Circuits and Systems for Video Technology*, Vol. 13, 2003, pp. 890-896.
12. M. Fallahpour, "Reversible image data hiding based on gradient adjusted prediction," *IEICE Electron*, Vol. 5, 2008, pp. 870-876.
13. Y. Hu, H. K. Lee, and J. Li, "DE-based reversible data hiding with improved overflow location map," *IEEE Transactions on Circuits and Systems for Video Technology*, Vol. 19, 2009, pp. 250-260.
14. Z. Ni, Y. Q. Shi, N. Ansari, and W. Su, "Reversible data hiding," *IEEE Transactions on Circuits and Systems for Video Technology*, Vol. 16, 2006, pp. 354-362.
15. Q. Ying, Z. Qian, and X. Zhang, "Reversible data hiding with image enhancement using histogram shifting," *IEEE Access*, Vol. 7, 2019, pp. 46506-46521.
16. L. Luo, Z. Chen, M. Chen, X. Zeng, and Z. Xiong, "Reversible image watermarking using interpolation technique," *IEEE Transactions on Information Forensics and Security*, Vol. 5, 2010, pp. 187-193.
17. Y. Jia, Z. Yin, and X. Zhang, "Reversible data hiding based on reducing invalid shifting of pixels in histogram shifting," *Signal Processing*, Vol. 163, 2019, pp. 238-246.
18. A. Kerckhoffs, *Journal des Sciences Militaires*, Vol. 9, 1883, pp. 5-38.
19. O. Kuznetsov, M. Lutsenko, and D. Ivanenko, "Strumok stream cipher: Specification and basic properties," in *Proceedings of IEEE 3rd International Scientific-Practical Conference Problems of Infocommunications Science and Technology*, 2016, pp. 59-62.

Fang Ren (任方) received his Ph.D. 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.

Ming-Yu Yu (于明宇) is currently pursuing the Master's degree in Cyberspace Security from Xi'an University of Posts and Communications, Shannxi. His research interests include informa-tion hiding, cover randomness and cryptography.

Hai-Yan Xiu (修海燕) received her BS 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 include information hiding and reversible data hiding.