Hindawi
Security and Communication Networks
Volume 2021, Article ID 5495941, 16 pages
https://doi.org/10.1155/2021/5495941

Research Article

Cryptographic Secrecy Analysis of Adaptive Steganographic Syndrome-Trellis Codes

Hansong Du,[1,2] **Jiufen Liu**,[1] **Yuguo Tian**,[1] **and Xiangyang Luo**[1,2]

[1]*The State Key Laboratory of Mathematical Engineering and Advanced Computing, Zhengzhou 450001, China*
[2]*The Province Key Laboratory of Cyberspace Situation Awareness Zhengzhou, Zhengzhou 450001, Henan Province, China*

Correspondence should be addressed to Xiangyang Luo; luoxy_ieu@sina.com

Received 9 June 2021; Accepted 17 July 2021; Published 28 July 2021

Academic Editor: Zhili Zhou

Compared with traditional steganography, adaptive steganography based on STC (Syndrome-Trellis Codes) has extremely high antidetection ability and has been a mainstream and hot research direction in the field of information hiding over the past decades. However, it is noted, in specific scenarios, that a small number of methods can extract data from STC-based adaptive steganography, indicating security risks related to such algorithms. In this manuscript, the cryptographic secrecy of this kind of steganography is analyzed, on condition of two common attacks: stego-only attack and known-cover attack, respectively, from three perspectives: steganographic key equivocation, message equivocation, and unicity distance of the steganographic key. Focusing on the special layout characteristics of the parity-check matrix of STC, under the two attack conditions, the theoretical boundaries of the steganographic key equivocation function, the message equivocation function, and the unicity distance of the steganographic key are separately obtained, showing the impact of the three elements: the submatrix size, the randomness of the data, and the cover object on the cryptographic secrecy of the STC-based adaptive steganography, resulting in a theoretical reference to accurately judge the cryptographic secrecy of such steganography and design more secure steganography methods.

1. Introduction

Digital steganography ensures data security by embedding data into multimedia files such as digital images, audio, videos, etc., for transmission [1]. This kind of communication conceals the fact that "communication is happening" and is highly deceptive, which has become a main method of covert communication and a research hotspot in the field of information security in recent years [2]. The security of steganography includes covert security and cryptographic secrecy. The covert security refers to antidetection performance of data, and the cryptographic secrecy refers to antiextraction performance of data [3]. At present, there have been a lot of research studies [4–6] on the antidetection performance, while relatively few research studies [7] on the antiextraction performance. The adaptive steganography based on STC (Syndrome-Trellis Codes) [8] has a high antidetection performance by embedding data into complex texture areas that are difficult to model and has been a mainstream direction in the field of information hiding in recent years. At present, many STC-based adaptive steganography algorithms [9–13] have been proposed. However, there have been a few studies [14–16] that could extract data from STC-based adaptive steganography in specific scenarios, indicating that such algorithms may have hidden security risks. Therefore, carrying out a comprehensive and in-depth cryptographic secrecy analysis of such steganography has important research value for judging the security of such steganography and designing more secure steganography methods.

Early studies on steganographic security mainly focused on the covert security. Cachin [17] was the first to study the covert security from the perspective of communication. He defined the active attacker and the passive attacker by the information theory model and distinguished the concepts of perfect concealment and perfect confidentiality for the first time. Hopper [18] studied the problem of covert security from the perspective of cryptography and defined covert

security from the perspective of computational complexity under the assumption of passive aggression. As the problem of data extraction was put forward, some scholars [3, 9–12] pointed out that steganography should not only have covert security but also have cryptographic secrecy.

Data extraction essentially is a kind of cryptanalysis [3]. Provos and Honeyman [19] first studied the cryptographic secrecy of steganography and proposed a general model for attacking random steganography, that is, simultaneously exhausting the encryption key and steganography key space. The computational complexity of the attack algorithm is $O(|K| \times |E|)$ where K represents the steganographic key space and E represents the encryption key space. Fridrich et al. [20, 21] analyzed the cryptographic secrecy for the first time from the perspective of computational complexity and pointed out that if an attacker could independently extract the data, the attack complexity of restoring plaintext could be reduced from $O(|K| \times |E|)$ to $O(\max\{|K|, |E|\})$. Zhang and Li [3] gave a measurement method of cryptographic secrecy and the relationship among cryptographic secrecy, information transmission rate, and key rate by drawing on Shannon's definition of the confidentiality system. In addition, he pointed out that the cryptographic secrecy brought by steganography was essentially a cryptographic feature. Further, Zhang and Li pointed out in [22] that even if the data embedded through steganography was unencrypted, it was still relatively secure in the sense of cryptography as long as the steganography itself had strong cryptographic secrecy.

With the proposal of a large number of steganography algorithms [23–25] based on matrix coding [26], the research on cryptographic secrecy has shifted to cryptographic secrecy of steganographic matrix coding. Regalia [27] used the information theory method to study the cryptographic secrecy of steganographic matrix coding under the condition of stego-only attack. The upper bound of the steganographic key equivocation function and the relationship among message equivocation function, cover entropy, and data entropy under different steganographic key models were separately obtained in [27]. In addition, Regalia demonstrated that the perfect secrecy defined by Shannon can be progressively achieved using wet paper coding. Chen et al. [28] studied the cryptographic secrecy of matrix coding under different attack conditions. In the condition of stego-only attack, the theoretical bound of unicity distance of the steganographic key was given, which supplemented the research results of Regalia. Under the condition of known-cover attack, the upper bounds of the steganographic key equivocation function and message equivocation function of matrix encoding-based steganography were given.

In recent years, STC-based adaptive steganography has become a research hotspot in the field of information hiding with high covert security [29]. This type of coding makes the data embedding related to all the elements of the image, resulting in a decrease in the correlation between the steganographic key and stego object, and has extremely high resistance to detection. However, in the existing literatures [14–16], there have been a small number of data extraction methods, which could extract data from STC-based adaptive steganography under specific conditions. Liu et al. [14] presented a "column grouping" method for extracting the data under the conditions of "chosen-stego-object" and "data-retransmission," respectively. These methods were based on the time-invariant property of the convolutional codes, and they could reduce the steganographic key space to a very small candidate set for arbitrary relative payload without exhaustive searches. In our previous research [15, 16], we presented a method for extracting data, respectively, in two cases where embedded data was plaintext and part of plaintext was known. Aiming at the case that embedded data was plaintext, Luo et al. [15] proposed an extraction method based on the parameter identification of STC. Based on the randomness difference between plaintext and ciphertext, the method first exhausted the submatrices and then judged whether the submatrix was correct or not according to the randomness of the data extracted from different submatrices. Under the condition that part of plaintext was known, Gan et al. [16] proposed a data extraction method based on the identity transformation of the decoding equation. This method used the identity deformation of the parity-check matrix operation to simplify the decoding equation, then converted the unknown and relatively complex parity-check matrix into a column vector that was easy to solve, and finally eliminated the impossible parity-check matrix based on the code judgment standard. The above research studies show that, in some cases, STC-based adaptive steganography may have hidden confidential dangers, and it is necessary for us to carry out research on the cryptographic secrecy of STC-based adaptive steganography. However, unlike general matrix coding, there are few research results on the cryptographic secrecy of STC-based adaptive steganography, and the element affecting the cryptographic secrecy is not clear yet. We still need to conduct in-depth analysis on the cryptographic secrecy of such algorithm to measure the cryptographic secrecy of such algorithms is related to what element and how are they related. To be specific, what are the upper bounds of the amount of data information and steganographic key information that can be leaked from stego objects and cover objects? What elements are the upper bounds relate to and in what relation? What is the lower bound of the amount of information an attacker needs to recover the steganographic key? What elements are this lower bound relate to and in what relation?

For this reason, this manuscript carries out the cryptographic secrecy research on STC-based adaptive steganography. Benchmarking the related theories in classical cryptography, this manuscript analyzes the cryptographic secrecy of steganography from three aspects, namely, the steganographic key equivocation, the message equivocation,

and the unicity distance of the steganographic key, under two attack conditions of stego-only and known-cover, respectively. The main work of this manuscript is as follows:

(1) Under the condition of stego-only attack, the cryptographic secrecy of STC-based adaptive steganography algorithm is studied from three aspects: the steganographic key equivocation, the message equivocation, and the unicity distance of the steganographic key. More specifically, under the condition of stego-only attack and based on the special structure of the STC parity-check matrix, we obtain the upper bound of the amount of steganographic key information and data information leaked from the stego object, the lower bound of the amount of information an attacker needs to recover the steganographic key, and the quantitative relationship between these theoretical bounds and submatrices, data, and cover objects. It can be seen from the obtained quantitative relationship: the better the randomness of the data and the cover object and the larger the scale of the STC submatrices, correspondingly the stronger the cryptographic secrecy.

(2) Under the condition of known-cover attack, the cryptographic secrecy of the STC-based adaptive steganography algorithm is studied from three aspects: the steganographic key equivocation, the message equivocation, and the unicity distance of the steganographic key. More specifically, under the condition of known-cover attack and based on the special structure of the STC parity-check matrix, we obtain the upper bound of the amount of steganographic key information and data information leaked from the stego object and cover object, the lower bound of the amount of information an attacker needs to recover the steganographic key, and the quantitative relationship between these theoretical bounds and submatrices, data, and cover objects. It can be seen from the obtained quantitative relationship: the better the randomness of the data and the cover object and the larger the scale of the STC submatrices, correspondingly the stronger the cryptographic secrecy.

The structure of this manuscript is as follows: Section 2 is a description of the problem, which introduces the notation used in this manuscript, analyzes the STC encoding and decoding principle, and puts forward the problems to be studied in this manuscript. This manuscript intends to study the cryptographic secrecy of STC-based adaptive steganography from three aspects: the steganographic key equivocation, the message equivocation, and the unicity distance of the steganographic key. Section 3 studies the theoretical bound of the steganographic key equivocation, the message equivocation, and the unicity distance of the steganographic key under the stego-only attack. Section 4 studies the theoretical bound of the steganographic key equivocation, the message equivocation, and the unicity distance of the steganographic key under known-cover attack. Section 5 is the discussion and conclusion of this manuscript.

2. Problem Setup

In this section, we will introduce the notation used in this manuscript, analyze the principle of STC encoding and decoding, and put forward the problems to be studied in this manuscript.

2.1. Symbols. In this manuscript, random variables are denoted by uppercase italic letters, with lowercase bold letters denoting particular realizations. Decorated letters denote the set. We treat all signals as vectors of bits (each 0 or 1), using componentwise modulo-2 addition over the Galois field F_2. In particular, X is the cover sequence of length n, Y is the stego sequence of length n, and M is the data of length of q, in which $q < n$.

Entropy is denoted by $H(\cdot)$, as in

$$H(X) = -\sum_{\mathbf{x}\in X} p(x)\log_2 p(\mathbf{x}). \tag{1}$$

The entropy is used to describe the average uncertainty of random variables. Assuming $X_1, X_2, \ldots, X_n$ are random variables, the joint entropy satisfies the chain rule:

$$H(X_1, X_2, \ldots, X_n) = \sum_{i=1}^{n} H(X_i|X_{i-1}, \ldots, X_1). \tag{2}$$

Conditional entropy is denoted by $H(X|Y)$, as in

$$H(X|Y) = \sum_{\mathbf{y}\in Y} p(\mathbf{y})H(X|Y=\mathbf{y}) = -\sum_{\mathbf{x}\in X}\sum_{\mathbf{y}\in Y} p(\mathbf{x},\mathbf{y})\log_2 p(\mathbf{y}|\mathbf{x}). \tag{3}$$

The conditional entropy is used to describe the average uncertainty of random variable Y under the condition of known random variable X.

Average mutual information is denoted by $I(X;Y)$, as in

$$I(M;Y) = H(M) - H(M|Y) = \sum_{\mathbf{m}\in M}\sum_{\mathbf{y}\in Y} p(\mathbf{m},\mathbf{y})\log_2\frac{p(\mathbf{m},\mathbf{y})}{p(\mathbf{m})p(\mathbf{y})}. \tag{4}$$

The average mutual information is used to describe how much uncertainty about random variable X can be eliminated when random variable Y is known.

2.2. Analysis of STC Encoding and Decoding Principle. This section will briefly analyze the principle of STC encoding and decoding in adaptive steganography. Before the analysis, we first introduce the basic process of STC-based adaptive steganography.

We begin with the basic setup of Figure 1. A binary cover sequence $\mathbf{x}$ is first extracted from a cover object (image, audio, videos, etc.) by a bit-assignment function which is commonly assumed publicly known. Thus, for simplicity, the cover

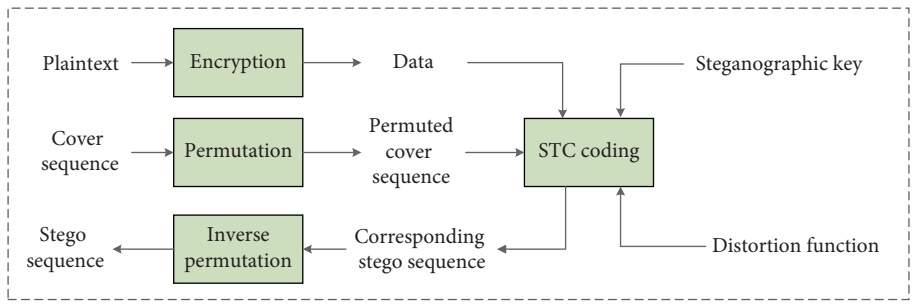

Figure 1: The data embedding process of STC-based adaptive steganography.

sequence and stego sequence can be thought as the cover and stego object in our analysis. Assume that both sides of communication want to transfer data $\mathbf{m}$ ($\mathbf{m} \in F_{2^q}$) with q bits, using a binary cover sequence $\mathbf{y}$ ($\mathbf{y} \in F_{2^n}$) whose length is n, where $q < n$. Usually, the data is encrypted ciphertext. The sender first permutes the binary cover sequence into the permuted cover sequence, then calculates the embedding distortion in different locations of the cover image, and finally uses STC to select the modifying positions adaptively according to the calculated distortion and embed data with minimum embedding distortion. After the sender inversely permuting the corresponding stego sequence, the stego sequence can be obtained.

In the above process, the STC is the most important. The following is an analysis of the STC encoding and decoding principle.

The cover object and stego object are denoted as $\mathbf{x} = (x_1, x_2, \ldots, x_n)$ and $\mathbf{y} = (y_1, y_2, \ldots, y_n) \in F_2^n$, respectively, where the embedded data is denoted as $\mathbf{m}$. The STC encoding and decoding processes can be realized by equations (5) and (6), respectively:

$$\mathbf{y} = \mathrm{Emb}(\mathbf{x}, \mathbf{m}) = \arg\min_{y \in C(\mathbf{m})} D(\mathbf{x}, \mathbf{y}), \tag{5}$$

$$\mathbf{m} = \mathrm{Ext}(\mathbf{y}) = \mathbf{k}\mathbf{y}, \tag{6}$$

where $D(\mathbf{x}, \mathbf{y})$ is an embedding distortion function, $\mathbf{k}$ and $\mathbf{k} \in F_2^{q \times n}$ is the STC parity-check matrix, and $C(\mathbf{m}) = \{\mathbf{z} \in F_2^n | \mathbf{k}\mathbf{z} = \mathbf{m}\}$ is the coset corresponding to syndrome. From equation (5), we can see that the purpose of STC encoding is to find the optimal $\mathbf{y}$ subjected to equation (6) to minimize embedding distortion $D(\mathbf{x}, \mathbf{y})$.

The parity-check matrix $\mathbf{k}$ is composed of a small submatrix $\mathbf{k}_1$ of size $h \times w$, as shown in Figure 2. The submatrices are placed next to each other and shifted down by one row. The values of the elements in the submatrix denote the encoding content parameters. The width w is dictated by the relative payload α. If the relative payload α is equal to $1/k$ for some $k \in Z^+$ (Z^+ represents the positive integer), then select $w = k$; otherwise, if $1/k + 1 < \alpha < 1/k$, then the parity-check matrix $\mathbf{k}$ will contain a mix of submatrices of widths k and $k + 1$.

For example, suppose the relative payload $\alpha = 0.5$, then the parity-check matrix $\mathbf{k}$ is composed of one submatrix $\mathbf{k}_1$. If the submatrix $\mathbf{k}_1$ is selected as $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$, then parity-check matrix $\mathbf{k}$ can be shown as

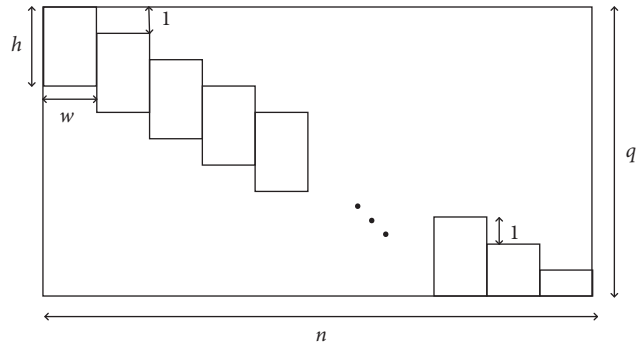

Figure 2: The structure of STC parity-check matrix.

$$\begin{pmatrix} 1 & 0 & & & & & & \\ 0 & 1 & 1 & 0 & & & & \\ & & 0 & 1 & 1 & 0 & & \\ & & & & 0 & 1 & \ddots & \\ & & & & & & 1 & 0 \\ & & & & & & 0 & 1 & 1 & 0 \end{pmatrix}. \tag{7}$$

If the relative payload $\alpha = 0.4$, then the parity-check matrix $\mathbf{k}$ is composed of two different submatrices. For example, if the submatrices are selected as $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ and $\begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & 1 \end{pmatrix}$, then parity-check matrix $\mathbf{k}$ will be formed as

$$\begin{pmatrix} 1 & 0 & & & & & & \\ 0 & 1 & 1 & 1 & 1 & & & \\ & & 0 & 1 & 1 & 1 & 0 & \\ & & & & 0 & 1 & \ddots & \\ & & & & & & 1 & 1 & 1 \\ & & & & & & 0 & 1 & 1 & 1 & 0 \end{pmatrix}. \tag{8}$$

As shown in Figure 1, the binary cover sequence is usually permuted into the permuted cover sequence before embedding the data in the actual covert communication based on adaptive steganography. Then, the sender uses STC encoding to embed the data into the permuted cover sequence to generate the corresponding stego sequence. Finally, perform the inverse permutation operation on the

corresponding stego sequence to generate the stego sequence and send it to the receivers. The receivers extract the data through the preappointed submatrices and permutation process. For attackers to obtain the content of covert communication, his task is to extract the embedded data from the intercepted stego objects. As long as the correct parity-check matrices and the process of permutation are obtained, the attackers can extract embedded data from STC-based adaptive steganography such as receivers. It is worth noting that the permutation process is mostly determined by the length of the data. As the same time, the length of the data is exactly the height of the parity-check matrix. In sum, if attackers obtain the correct parity-check matrices, he can be the same as the receivers and extract the data from STC-based adaptive steganography. Therefore, the extraction of data from STC-based adaptive steganography is equivalent to the recovery of parity-check matrices. From this perspective, we can regard the parity-check matrices as the steganographic key in the covert communication process.

Shannon [30] pointed out that "breaking a good cryptographic system" is equivalent to solving a complex equation that contains a large number of unknowns. However, it can be seen from the above analysis that the decoding system of STC is a system of linear equations, whose form is simple (the parity-check matrix is simply rearranged of the submatrices in the main diagonal direction of the parity-check matrix) and vulnerable to attack.

In this manuscript, cryptographic secrecy of STC-based adaptive steganography is analyzed under two common attack conditions: stego-only and known-cover. The stego-only attack refers to the steganographic key recovery under the condition that only the stego object is obtained; the known-cover attack refers to the steganographic key recovery under the condition that the stego object and cover object are obtained. From Figure 1, we can see that the parity-check matrix, distortion function, data, and cover object are the four elements in the embedding process of STC-based adaptive steganography. What is the relationship between the cryptographic secrecy of STC-based adaptive steganography and submatrix, distortion function, data, stego object, and cover object? More specifically, under the two conditions, what is the upper bound of the amount of steganographic key information and data information leaked from the stego object and cover object? What does this upper bound have to do with the submatrix, distortion function, data, stego object, and cover object? What is the lower bound of the information required by the attacker to recover the steganographic key under these attack conditions? What does this lower bound have to do with the submatrix, distortion function, data, stego object, and cover object? These are the questions to be studied in this manuscript.

3. Cryptographic Secrecy of STC under Stego-Only Attack

The most common scenario is that the attacker only obtains the stego object. We call this steganographic key recovery under that condition as the stego-only attack, which is the most difficult and common type of all attacks. In the following, we are concerned about the upper bound of the amount of the steganographic key information and data information that can be leaked by the stego object, and the lower bound of the amount of information required by the attacker to recover the steganographic key under this attack condition.

3.1. Steganographic Key Equivocation. Under the stego-only attack, the steganographic key equivocation function is denoted by $I(K;Y)$ [27] as in

$$I(K;Y) = \sum_{\mathbf{k}\in F_2^{q\times n}} \sum_{\mathbf{y}\in F_2^n} p(\mathbf{k},\mathbf{y}) \log \frac{p(\mathbf{k},\mathbf{y})}{p(\mathbf{k})p(\mathbf{y})}, \tag{9}$$

which measures how much steganographic key information may be revealed from observation of the stego object. The greater the steganographic key equivocation function $I(K;Y)$, the more steganographic key information can be obtained by the attacker from the stego object, that is, the easier the attacker can infer the correct steganographic key and the less secure the steganographic system will be. The following theorem gives the upper bound of the steganographic key equivocation function under the stego-only attack, that is, how much steganographic key information can be leaked by the stego object at most.

Theorem 1. *Under the stego-only attack, when all cover objects and data equally probable, the key equivocation function is bounded as*

$$I(K;Y) \le [q - H(M)] + [n - H(X)], \tag{10}$$

in which q is the length of data M.

Proof. According to the chain rule of the entropy function (equation (2)), we can isolate the joint entropy $H(X,M,Y,K,T)$ of cover object X, data M, stego object Y, steganographic key K, and distortion function T as follows:

$$H(X,M,Y,K,T) = H(K,M,T,X) + H(Y|K,M,T,X). \tag{11}$$

According to equation (5), the sender in covert communication can generate a unique stego object Y from the steganographic key K, data M, distortion function T, and cover object X, which implies

$$H(Y|K,M,T,X) = 0. \tag{12}$$

Following equation (11), we have

$$H(X,M,Y,K,T) = H(K,M,T,Y) + H(Y \mid K,M,T,X) = H(K,M,T,X) = H(K) + H(M) + H(T) + H(X). \tag{13}$$

The last step is valid since the independence of the steganographic keys K, stego object Y, distortion function T, and cover object X. According to the chain rule of the entropy function (equation (2)), we can isolate the entropy $H(X,M,Y,K,T)$ in another way:

$$H(X,M,Y,K,T) = H(Y) + H(K \mid Y) + H(M|K,Y) + H(T \mid M,K,Y) + H(X \mid M,K,Y,T). \tag{14}$$

Combining equations (13) and (14), we get

$$I(K;Y) = H(Y) - H(M) - I(T;M,K,Y) - I(X;M,T,Y,K) = H(Y) - H(M) - I(T;K,Y) - I(X;K,Y,T). \tag{15}$$

According to the relationship between mutual information and entropy (equation (4)), the average mutual information $I(X;K,Y,T)$ can be isolated as follows:

$$I(X;K,Y,T) = H(X) - H(X|K,Y,T). \tag{16}$$

By substituting equation (16) into equation (15), we get

$$H(X|K,Y,T) = I(K;Y) + I(T;K,Y) - H(Y) + H(M) + H(X). \tag{17}$$

According to equation (2), we can isolate the entropy joint $H(Y,X,T,K,M)$ as follows:

$$H(Y,X,T,K,M) = H(X|T,Y,K,M) + H(M|T,K,Y) + H(T,K,Y). \tag{18}$$

The independence between distortion function T, steganographic key K, and stego object Y means

$$H(T,K,Y) = H(T) + H(K) + H(Y). \tag{19}$$

Substitute equation (19) into equation (18), we get

$$H(Y,X,T,K,M) = H(X \mid T,Y,K,M) + H(M \mid T,K,Y) + H(T) + H(K) + H(Y) = H(X \mid T,Y,K,M) + +H(T) + H(K) + H(Y). \tag{20}$$

From equation (6), we know that the data M can be obtained by the steganographic key K and the stego object Y, suggesting $H(M|T,K,Y) = 0$. As a result, the last step is valid.

We can isolate the entropy joint $H(Y,X,T,K,M)$ in another way:

$$H(Y,X,T,K,M) = H(Y \mid X,T,K,M) + H(X,T,K,M). \tag{21}$$

The independence between cover object X, distortion function T, steganographic key K, and data M means

$$H(X,T,K,M) = H(X) + H(T) + H(K) + H(M). \tag{22}$$

Substitute equation (22) into equation (21), we get

$$H(Y,X,T,K,M) = H(Y|X,T,K,M) + H(X) + H(T) + H(K) + H(M) == H(X) + H(T) + H(K) + H(M). \tag{23}$$

From equation (5), we know that the stego object Y can be obtained by the cover object X, distortion function T, steganographic key K, and data M, suggesting $H(Y|X,T,K,M) = 0$. As a result, the last step is valid. Combining equations (20) and (23), we get

$$H(X \mid T,Y,K,M) = H(X) - H(Y) + H(M). \tag{24}$$

Now, if $H(X) = n$ (all cover objects are equally probable) and $H(M) = q$ (all data are equally probable), then

$$H(X|T,Y,K) = H(X|T,Y,K,M) = n + q - H(Y), \tag{25}$$

in which $H(X \mid T,Y,K,M) = H(X \mid T,Y,K)$ is an application of equation (6). By substituting equation (25) into equation (17), we get

$$I(K;Y) + I(T;K,Y) = [q - H(M)] + [n - H(X)]. \tag{26}$$

Together with nonnegative of average mutual information, we get the desired result.

Particularly, when all cover objects and data are equally probable, that is, $H(M) = q$ and $H(X) = n$, the following equation is obtained:

$$I(K;Y) + I(T;K,Y) = 0. \tag{27}$$

Then, an application of the nonnegative of average mutual information yields

$$\begin{aligned} I(K;Y) &= 0, \\ I(T;K,Y) &= n. \end{aligned} \tag{28}$$

Theorem 1 shows that the knowledge of the stego object does not assist in deducing the uncertainty of steganographic key ($I(K;Y) = 0$) when the data is completely random ($H(M) = q$) and cover object is completely random ($H(X) = n$). This means (1) the choice of cover has an impact on cryptographic secrecy of STC-based adaptive steganography. The better the randomness of cover, the higher the cryptographic secrecy. (2) Compared to the data is plaintext, when the data is encrypted ciphertext, the cryptographic secrecy of STC-based adaptive steganography is higher.

It is worth noting that, as a result of Theorem 1, the upper bound on the steganographic key equivocation function is independent of the distortion function, that is, the uncertainty about the steganographic key is independent of the specific distortion function taken by the adaptive steganographic algorithm. However, most of the existing studies on steganographic algorithms are in pursuit of the design of new distortion functions, which may improve the covert security, that is, antidetection, but is not conducive to the enhancement of cryptographic secrecy. □

3.2. Message Equivocation. Under the stego-only attack, the message equivocation function is denoted by $I(M;Y)$ as in

$$I(M;Y) = \sum_{\mathbf{m}\in F_2^q} \sum_{\mathbf{y}\in F_2^n} p(\mathbf{m},\mathbf{y}) \log \frac{p(\mathbf{m},\mathbf{y})}{p(\mathbf{m})p(\mathbf{y})}, \tag{29}$$

which measures how much data information may be revealed from observation of the stego object. The greater the message equivocation function is, the more data information can be obtained by the attacker from the stego object, that is, the easier the attacker can extract the data, and the less secure the steganographic system will be. The following theorem gives the upper bound of the message equivocation function under the stego-only attack, that is, how much data information can be leaked by the stego object at most.

In order to establish a relationship between the upper bound of message equivocation function $I(M;Y)$ and the size of the submatrix, we first prove the following lemma.

Lemma 1. *When the reciprocal of the relative payload α is an integer, the STC parity-check matrix consists of a single submatrix with a width of w_1; then, the conditional entropy $H(K|Y)$ is*

$$H(K|Y) = \sum_{j=0}^{w_1-1} \log\left(2^{h-2} - j\right). \tag{30}$$

When the reciprocal of the relative payload α is not an integer, the STC parity-check matrix consists of two submatrices with widths w_1 and w_2. Then, the conditional entropy $H(K|Y)$ is

$$H(K|Y) = \sum_{i=1}^{2} \sum_{j=0}^{w_i-1} \log\left(2^{h-2} - j\right), \tag{31}$$

in which $w_1 = 1/\alpha$ and $w_2 = 1/\alpha + 1$.

Proof. According to the stego object, we can estimate the relative payload α. For example, in [31], the rich model is used for quantitative analysis to realize the estimation of relative payload α. The width of the submatrix can be obtained by relative payload α. For a submatrix with height h and width w, the number of all possible submatrices is 2^{hw}. Filler et al. [8] pointed out that a good submatrix should meet the requirements that the first row and the last row are 1 and any two columns are not the same. When the reciprocal of the relative payload is an integer, the parity-check matrix is only composed of a single submatrix, and the size of the steganographic key space is $|K| = A_{2^{h-2}}^{w}$, in which $A_m^n = m!/(m-n)!$. Therefore, given the stego object, the average uncertainty of the steganographic key is

$$H(K|Y) = \sum_{i=1}^{A_{2^{h-2}}^{w_1}} \frac{1}{A_{2^{h-2}}^{w_1}} \log_2 A_{2^{h-2}}^{w_1} = \log_2 A_{2^{h-2}}^{w_1} = \sum_{j=0}^{w_1-1} \log_2\left(2^{h-2} - j\right). \tag{32}$$

The penultimate step is valid since $\log_2(A_{2^{h-2}}^{\mathrm{w}}) = \log_2((2^{h-2}) \times (2^{h-2}-1) \times \cdots (2^{h-2} - \mathrm{w} + 1)) = \sum_{j=0}^{w-1} \log_2 (2^{h-2} - j)$.

The parity-check matrix is composed of two submatrices when the reciprocal of the relative payload is not an integer. The size of the steganographic key space is

$$|K| = A_{2^{h-2}}^{w_1} \times A_{2^{h-2}}^{w_2}. \tag{33}$$

Thus,

$$\begin{aligned} H(K|Y) &= \sum_{i=1}^{A_{2^{h-2}}^{w_1} \times A_{2^{h-2}}^{w_2}} \frac{1}{A_{2^{h-2}}^{w_1} \times A_{2^{h-2}}^{w_2}} \log_2\left(A_{2^{h-2}}^{w_1} \times A_{2^{h-2}}^{w_2}\right) \\ &= \log_2\left(A_{2^{h-2}}^{w_1} \times A_{2^{h-2}}^{w_2}\right) \\ &= \sum_{j=0}^{w_1-1} \log_2\left(2^{h-2} - j\right) + \sum_{j=0}^{w_2-1} \log_2\left(2^{h-2} - j\right) \\ &= \sum_{i=1}^{2} \sum_{j=0}^{w_i-1} \log_2\left(2^{h-2} - j\right), \end{aligned} \tag{34}$$

in which $w_1 = 1/\alpha$ and $w_2 = 1/\alpha + 1$. The penultimate step is valid since $\log_2(A^{w}_{2^{h-2}}) = \log_2((2^{h-2}) \times (2^{h-2} - 1) \times \cdots (2^{h-2} - w + 1)) = \sum_{j=0}^{w-1} \log_2(2^{h-2} - j)$.

For example, when the height of the submatrix is fixed at 7, the relationship between $H(K|Y)$ and the relative payload α is shown in Figure 3. When the number of different submatrices is fixed at one (that is, the reciprocal of the relative payload is an integer), the relative payload is taken as 0.05 bpp, 0.1 bpp, 0.2 bpp, 0.25 bpp, and 0.5 bpp. When the number of different submatrices is fixed at two (that is, when the reciprocal of the relative payload is not an integer), the relative payload is taken as 0.06 bpp, 0.15 bpp, 0.24 bpp, 0.35 bpp, and 0.45 bpp. It can be seen from Figure 3 that $H(K|Y)$ decreases as the relative payload increases when the number of different submatrices is fixed. The relationship between $H(K|Y)$ and the height of the submatrix is shown in Figure 4. The relative payload is fixed at 0.2 bpp and 0.4 bpp in order. When the relative payload is fixed at 0.2 bpp, the parity-check matrix is composed of one submatrix with width of 5; when the relative payload is fixed at 0.4 bpp, the parity-check matrix is composed of two different submatrices with width of 2 and 3. It can be seen from Figure 4 that $H(K|Y)$ increases as the height of the submatrix increases when the relative payload is fixed.

Lemma 1 indicates the relationship between conditional entropy $H(K|Y)$ and the size of submatrices. Based on this relationship, we can obtain the relationship between the upper bound of the message equivocation function and the size of the submatrices under the stego-only attack. See the following theorem for details.

Theorem 2. *Under the condition of stego-only attack, the message equivocation function is bounded as*

$$I(M;Y) \le H(Y) - H(K) + H(K|Y), \tag{35}$$

in which $H(K|Y) = \sum_{j=0}^{w_1-1} og(2^{h-2} - j)$ *when the STC parity-check matrix consists of a single submatrix with a width of* w_1*;* $H(K|Y) = \sum_{i=1}^{2} \sum_{j=0}^{w_i-1} log(2^{h-2} - j)$ *when the STC parity-check matrix consists of two submatrices with widths* w_1 *and* w_2*.*

Proof. Due to the relationship between mutual information and entropy, we have

$$I(M;Y) = H(M) - H(M|Y). \tag{36}$$

Combining equations (13) and (14), we get

$$\begin{aligned} H(M) = {} & H(Y) + H(K|Y) + H(T|M,K,Y) \\ & + H(X|M,K,Y,T) - H(K) - H(T) - H(X), \end{aligned} \tag{37}$$

and substituting (37) into (36), we get

$$I(M;Y) = H(Y) - H(K) - H(T) - H(X) + H(T|M,K,Y) + H(X|M,K,Y,T) + H(K|Y) - H(M|Y). \tag{38}$$

Due to the chain rule of the entropy function (equation (2)), the joint entropy $H(M,K,Y)$ can be isolated in two ways:

$$H(M,K,Y) = H(Y) + H(M|Y) + H(K|M,Y), \tag{39}$$

$$\begin{aligned} H(M,K,Y) &= H(Y) + H(K|Y) + H(M|K,Y) \\ &= H(Y) + H(K|Y). \end{aligned} \tag{40}$$

Combining equation (39) with (40), we have

$$H(K|Y) - H(M|Y) = H(K|M,Y). \tag{41}$$

Substituting equation (41) into (38), we get

$$\begin{aligned} I(M;Y) &= H(Y) - H(X) - H(K) - H(T) + H(T|M,K,Y) + H(X|M,K,Y,T) + H(K|M,Y) \\ &= H(Y) - I(K;M,Y) - I(X;M,K,Y,T) - I(T;M,K,Y) \quad < H(Y) - I(K;M,Y). \end{aligned} \tag{42}$$

The penultimate step is valid because of an application of equation (4), and the last step is valid since mutual information is nonnegative.

Then, $I(K;M,Y) \ge I(K;Y)$ yields

$$\begin{aligned} I(M;Y) &\le H(Y) - I(K;M,Y) \\ &= H(Y) - I(K;Y) \\ &= H(Y) - H(K) + H(K|Y), \end{aligned} \tag{43}$$

in which $H(K|Y) = \sum_{j=0}^{w_1-1} \log(2^{h-2} - j)$ when the STC parity-check matrix consists of a single submatrix with a width of w_1; $H(K|Y) = \sum_{i=1}^{2} \sum_{j=0}^{w_i-1} \log(2^{h-2} - j)$ when the STC parity-check matrix consists of two submatrices with widths w_1 and w_2.

It can be seen from Theorem 2 that the upper bound of the message equivocation function increases as the height of the submatrices increases when the relative payload is fixed. When the number of different submatrices is fixed, the upper bound of the message

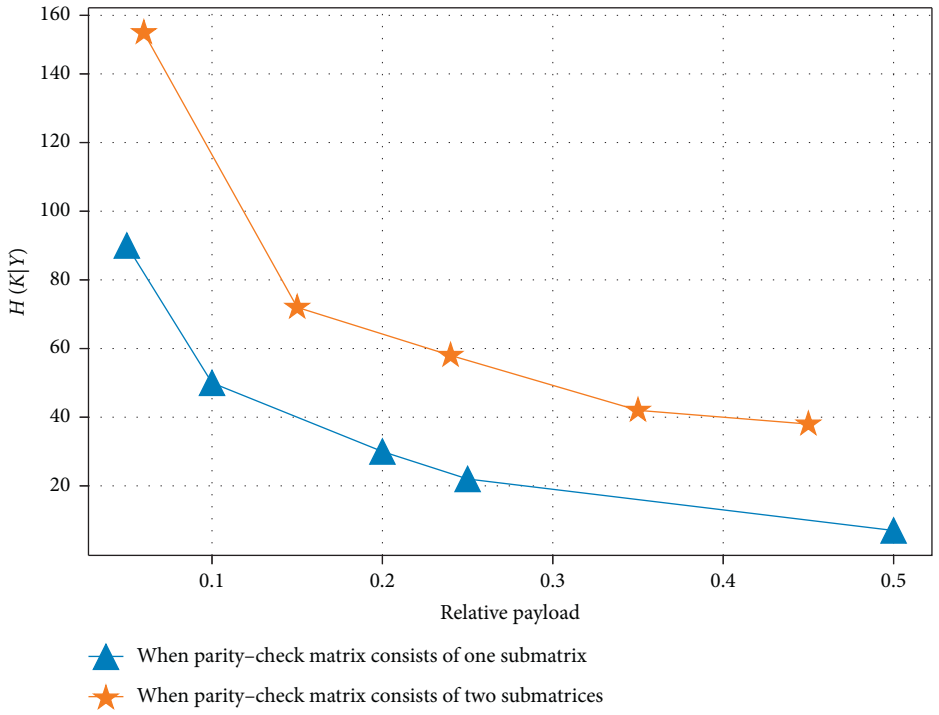

Figure 3: The relationship between $H(K|Y)$ and α.

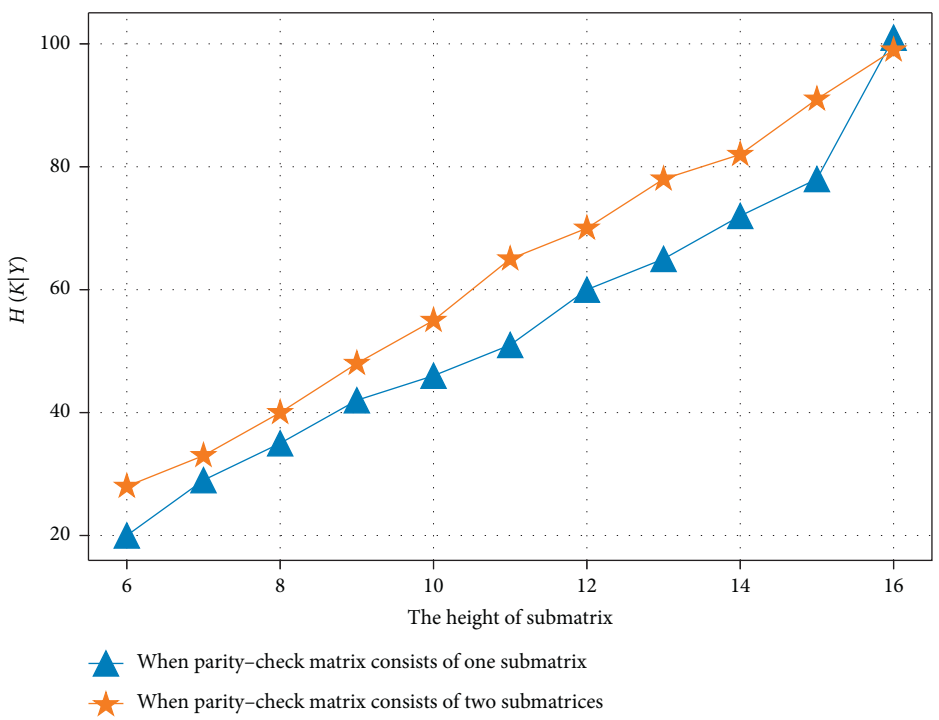

Figure 4: The relationship between $H(K|Y)$ and h.

equivocation function decreases as the relative payload increases. This is because the larger the submatrices size and the larger number of different submatrices mean the more encoding content parameters and harder to extract the data. Therefore, we should choose submatrices with bigger size and a relative payload whose reciprocal is not

an integer preferentially. However, the above methods will increase the time consumption of generating stego objects.

3.3. The Unicity Distance of the Steganographic Key. The security of a steganographic algorithm is generally only based on the secrecy of the steganographic key. Accordingly, a complete breach of a steganographic algorithm by an attacker means that he can find a way to recover the steganographic key. Therefore, the following is to further analyze the cryptographic secrecy of STC-based adaptive steganography from the perspective of the unicity distance of the steganographic key [3]. Specifically, we consider the minimum amount of data required by the attacker to recover the steganographic key on average. The following theorem gives the relationship between the unicity distance of the steganographic key N_K and the size of the submatrix under the stego-only attack.

Theorem 3. *Under the stego-only attack, the unicity distance of the steganographic key N_K is bounded as*

$$N_K \geq \frac{H(K|Y)}{H(Y) - [H(M) + I(T;K,Y) + I(X;K,Y,T)]}, \tag{44}$$

in which $H(K|Y) = \sum_{j=0}^{w_1-1} \log(2^{h-2} - j)$ when the STC parity-check matrix consists of a single submatrix with a width of w_1; $H(K|Y) = \sum_{i=1}^{2} \sum_{j=0}^{w_i-1} \log(2^{h-2} - j)$ when the STC parity-check matrix consists of two submatrices with widths w_1 and w_2.

Proof. Denote N_K groups of stego objects as $Y^{N_K} = \{Y_1, Y_2, \ldots Y_{N_K}\}$. Given N_K stego objects, then the set of all the possible steganographic keys $\mathscr{K}(Y^{N_K})$ is

$$\mathscr{K}\left(Y^{N_K}\right) = \{k \in K | \exists m_i \in M, s.t. pr(m_i) > 0, ky_i = m_i\}, \tag{45}$$

and the expectation of the number of pseudokeys $\overline{K}_P$ is

$$\overline{K}_P = \sum_{Y^{N_K}} \Pr\left(Y^{N_K}\right)\left[\left|\mathscr{K}\left(Y^{N_K}\right)\right| - 1\right] = \sum_{Y^{N_K}} \Pr\left(Y^{N_K}\right)|\mathscr{K}\left(Y^{N_K}\right)|-1, \tag{46}$$

where $|\mathscr{K}(Y^{N_K})|$ represents the number of elements in set $\mathscr{K}(Y^{N_K})$.

Then, an application of equation (3) yields

$$H\left(K|Y^{N_K}\right) = \sum_{Y^N} \Pr\left(Y^{N_K}\right) H\left(K|\left(Y^{N_K}\right)\right) = \sum_{Y^N} \Pr\left(Y^{N_K}\right) log_2 \left|\mathscr{K}\left(Y^{N_K}\right)\right| \leq \log_2 \left|\sum_{Y^N} \Pr\left(Y^{N_K}\right)\left|\mathscr{K}\left(Y^{N_K}\right)\right|\right| \leq \log(\overline{K}_P + 1), \tag{47}$$

and with equation (17), this yields

$$H\left(K|Y^{N_K}\right) = H(K) + N_K[H(M) - H(Y) + I(T;K,Y) + I(X;K,Y,T)]. \tag{48}$$

Together with equations (47) and (48), we get

$$\log\left(\overline{K}_p + 1\right) \leq H(K) + N_K[H(M) - H(Y) + I(T;K,Y) + I(X;K,Y,T)], \tag{49}$$

and the expectation of the number of pseudokeys N_K is bounded as

$$\overline{K}_p \leq 2^{H(K)+N_K[H(M)-H(Y)+I(T;K,Y)+I(X;K,Y,T)]} - 1. \tag{50}$$

On that account, the unicity distance is bounded as

$$N_K = \frac{H(K)}{H(Y) - [H(M) + I(T;K,Y) + I(X;K,Y,T)]} \geq \frac{H(K|Y)}{H(Y) - [H(M) + I(T;K,Y) + I(X;K,Y,T)]}, \tag{51}$$

in which $H(K|Y) = \sum_{j=0}^{w_1-1} \log(2^{h-2} - j)$ when the STC parity-check matrix consists of a single submatrix with a width of w_1; $H(K|Y) = \sum_{i=1}^{2} \sum_{j=0}^{w_i-1} \log(2^{h-2} - j)$ when the STC parity-check matrix consists of two submatrices with widths w_1 and w_2.

It can be seen from Theorem 6 that when the relative payload is fixed, the lower bound of the unicity distance of the steganographic key N_K increases as the height h of the submatrix increases; when the number of different submatrices is fixed, the unicity distance of the steganographic key N_K decreases as the relative payload α increases. This is because the larger sizes of submatrices and number of different submatrices mean the more encoding content parameters, that is, the more difficult it is to restore the steganographic key. Therefore, in order to recover the steganographic key, the average amount of information the attacker needs to obtain in advance become more. We should choose submatrices with bigger size and a relative payload whose reciprocal is not an integer preferentially. However, the above method will increase the time consumption of generating stego objects.

In this section, the cryptographic secrecy of the STC-based adaptive steganography algorithm is studied from three aspects: the steganographic key equivocation, the message equivocation, and the unicity distance of the steganographic key under the known-cover attack. More specifically, we obtain the upper bound of the amount of steganographic key information and data information

leaked from the cover object and stego object, the lower bound of the amount of information an attacker needs to recover the steganographic key, and the quantitative relationship between these theoretical bounds and the submatrices, data, and cover object.

4. Cryptographic Secrecy of STC under Known-Cover Attack

With the development of steganalysis technology, attackers may obtain stronger attack conditions: obtaining the cover object. Attack under this condition is called known-cover attack. Similar to Section 3, this section discusses the cryptographic secrecy of STC-based adaptive steganography from three aspects: the steganographic key equivocation function, message equivocation function, and unicity distance of the steganographic key.

4.1. Steganographic Key Equivocation. Under the known-cover attack, the steganographic key equivocation function is denoted by $I(K;X,Y)$ [27] as in

$$I(K;X,Y)=\sum_{\mathbf{k}\in F_2^{q\times n}}\sum_{\mathbf{x},\mathbf{y}\in F_2^n}p(\mathbf{k},\mathbf{x},\mathbf{y})\log\frac{p(\mathbf{k},\mathbf{x},\mathbf{y})}{p(\mathbf{k})p(\mathbf{x},\mathbf{y})}, \quad (52)$$

which measures how much steganographic key information may be revealed from observations of the cover object and stego object. The greater the steganographic key equivocation function is, the more steganographic key information can be obtained by the attacker from the cover object and stego object, that is, the easier the attacker can infer the steganographic key, and the less secure the steganographic system will be. The following theorem gives the upper bound of the steganographic key equivocation function under the known-cover attack, that is, how much steganographic key information can be leaked by the cover object and stego object at most.

Theorem 4. *Under the known-cover attack, the steganographic key equivocation function satisfies*

$$I(K;X,Y)=[H(Y|X)-H(M)]-I(T;X,Y,K), \quad (53)$$

in which $H(K|Y)=\sum_{j=0}^{w_1-1}\log(2^{h-2}-j)$ *when the STC parity-check matrix consists of a single submatrix with a width of* w_1*;* $H(K|Y)=\sum_{i=1}^{2}\sum_{j=0}^{w_i-1}\log(2^{h-2}-j)$ *when the STC parity-check matrix consists of two submatrices with widths* w_1 *and* w_2*.*

Proof. According to the chain rule of entropy function (equation (2)), joint entropy $H(Y,K,M,T,X)$ of the stego object Y, steganographic key K, data M, distortion function T, and cover object X can be isolated as

$$\begin{aligned}H(Y,K,M,T,X)&=H(K,M,T,X)+H(Y|K,M,T,X)\\&=H(K,M,T,X)\\&=H(K)+H(M)+H(X)+H(T).\end{aligned} \quad (54)$$

The penultimate step is valid because of an application of equation (12). The last step is valid since the independence of the steganographic key K, data M, distortion function T, and cover object X.

At the same time, the joint entropy $H(Y,K,M,T,X)$ can be rearranged as

$$\begin{aligned}H(Y,K,M,T,X)&=H(Y)+H(X|Y)+H(K|X,Y)+H(M|K,X,Y)+H(T|K,X,Y,M)\\&=H(Y)+H(X|Y)+H(K|X,Y)+H(T|K,X,Y,M).\end{aligned} \quad (55)$$

The last step is valid since equation (6) suggests $H(M|K,X,Y)=0$.

Combining equations (54) and (55), we get

$$H(K)+H(M)+H(X)+H(T)=H(Y)+H(X|Y)+H(K|X,Y)+H(T|K,X,Y,M). \quad (56)$$

That is,

$$[H(X)-H(X|Y)]+[H(K)-H(K|X,Y)]+[H(T)-H(T|K,X,Y,M)=H(Y)-H(M)]. \quad (57)$$

According to the relationship between mutual information and entropy (equation (4)), we have

$$I(Y;X) = H(X) - H(X|Y), \tag{58}$$

$$I(K;X,Y) = H(K) - H(K|X,Y), \tag{59}$$

$$I(Y;X) = H(X) - H(X|Y). \tag{60}$$

Substituting equations (58)–(60) into (57), we have

$$I(Y;X) + I(K;Y,X) + I(T;K,X,Y,M) = H(Y) - H(M). \tag{61}$$

That is,

$$\begin{aligned} I(K;X,Y) &= H(Y) - H(M) - I(Y;X) - I(T;K,X,Y,M) \\ &= H(Y|X) - H(M) - I(T;K,X,Y), \end{aligned} \tag{62}$$

in which $H(K|Y) = \sum_{j=0}^{w_1-1} \log(2^{h-2} - j)$ when the STC parity-check matrix consists of a single submatrix with a width of w_1; $H(K|Y) = \sum_{i=1}^{2} \sum_{j=0}^{w_i-1} \log(2^{h-2} - j)$ when the STC parity-check matrix consists of two submatrices with widths w_1 and w_2.

It can be seen from Theorem 4 that when the relative payload is fixed, the steganographic key equivocation function increases as the height of the submatrices increases; when the number of different submatrices is fixed, the steganographic keys' equivocation function decreases as the relative payload increases. This is because the larger the submatrices size and the more different submatrices number mean the more encoding content parameters and the more difficult to completely restore the steganographic key. Therefore, we should choose submatrices with bigger size, and a relative payload whose reciprocal is not an integer preferentially. However, the above methods will increase the time consumption of generating stego objects.

4.2. Message Equivocation. Under the known-cover attack, the message equivocation function is denoted by $I(M;X,Y)$ [28] as in

$$I(M;X,Y) = \sum_{\mathbf{m}\in F_2^q} \sum_{\mathbf{x},\mathbf{y}\in F_2^n} p(\mathbf{m},\mathbf{x},\mathbf{y}) \log_2 \frac{p(\mathbf{m},\mathbf{x},\mathbf{y})}{p(\mathbf{m})p(\mathbf{x},\mathbf{y})}, \tag{63}$$

which measures how much data information may be revealed from observations of the cover object and stego object. The greater the message equivocation function $I(M;X,Y)$ is, the more information about the data M can be obtained by the attacker from the cover object X and stego object Y, that is, the easier the attacker can extract the data, and the less secure the steganographic system will be. The following theorem gives the upper bound of the message equivocation function under the known-cover attack, that is, how much data information can be leaked by the cover object and stego object at most.

Theorem 5. *Under the known-cover attack, the message equivocation function $I(M;X,Y)$ is bounded as*

$$I(M;X,Y) \le H(Y|X) + H(K|Y) - H(K) - I(T;X,Y), \tag{64}$$

in which $H(K|Y) = \sum_{j=0}^{w_1-1} \log(2^{h-2} - j)$ when the STC parity-check matrix consists of a single submatrix with a width of w_1; $H(K|Y) = \sum_{i=1}^{2} \sum_{j=0}^{w_i-1} \log(2^{h-2} - j)$ when the STC parity-check matrix consists of two submatrices with widths w_1 and w_2.

Proof. According to the chain rule of entropy function (equation (2)), we can isolate the joint entropy $H(Y,K,M,T,X)$ in two ways:

$$\begin{aligned} H(Y,K,M,T,X) &= H(X) + H(Y|X) + H(M|X,Y) \\ &\quad + H(K|M,X,Y) + H(T|M,X,Y,K), \end{aligned} \tag{65}$$

$$H(Y,K,M,T,X) = H(X) + H(K) + H(M) + H(T). \tag{66}$$

Combining equations (63) and (64), we have

$$\begin{aligned} H(M) - H(M|X,Y) &= H(Y|X) + H(K|M,X,Y) \\ &\quad + H(T|M,X,Y,K) - H(T) - H(K). \end{aligned} \tag{67}$$

That is,

$$I(M;X,Y) = H(Y|X) - I(K;M,X,Y) - I(T;M,X,Y,K). \tag{68}$$

$I(K;M,X,Y) \ge I(K;X,Y)$ and $I(T;M,X,Y,K) \ge I(T;X,Y)$ yield

$$\begin{aligned} I(M;X,Y) &\le H(Y|X) - I(K;Y) - I(T;X,Y) \\ &= H(Y|X) + H(K|Y) - [H(K) + I(T;X,Y)], \end{aligned} \tag{69}$$

in which $H(K|Y) = \sum_{j=0}^{w_1-1} \log(2^{h-2} - j)$ when the STC parity-check matrix consists of a single submatrix with a width of w_1; $H(K|Y) = \sum_{i=1}^{2} \sum_{j=0}^{w_i-1} \log(2^{h-2} - j)$ when the STC parity-check matrix consists of two submatrices with widths w_1 and w_2.

It can be seen from Theorem 5 that when the relative payload is fixed, the message equivocation function increases as the height of the submatrix increases; when the number of different submatrices is fixed, the message equivocation function decreases as the relative payload increases. This is because the larger the submatrices size and number of different submatrices mean the more encoding content parameters and more difficult to extract the data completely. Therefore, we should choose submatrices with bigger size, and a relative payload whose reciprocal is not an integer preferentially. However, the above methods will increase the time consumption of generating stego objects.

4.3. The Unicity Distance of the Steganographic Key. The following theorem gives the relationship between the unicity distance of the steganographic key and the size of the submatrix under the cover-known attack.

Theorem 6. *Under the known-cover attack, the unicity distance of the steganographic key N_K is bounded as*

$$N_K \geq \frac{H(K|Y)}{H(Y|X) - [H(M) + I((T;Y,X,K))]}, \tag{70}$$

in which $H(K|Y) = \sum_{j=0}^{w_1-1} log(2^{h-2} - j)$ when the STC parity-check matrix consists of a single submatrix with a width of w_1; $H(K|Y) = \sum_{i=1}^{2} \sum_{j=0}^{w_i-1} log(2^{h-2} - j)$ when the STC parity-check matrix consists of two submatrices with widths w_1 and w_2.

Proof. Denote N_K groups of covers and stego objects as $X^{N_K} = \{X_1, X_2, \ldots, X_{N_K}\}$ and $Y^{N_K} = \{Y_1, Y_2, \ldots Y_{N_K}\}$.

Given N_K pairs of covers and stego objects, then denote the set of all the possible steganographic keys K as $\mathscr{K}(Y^{N_K}, X^{N_K})$; then,

$$\mathscr{K}\left(Y^{N_K}, X^{N_K}\right) = \{\mathbf{k} \in K | \exists \mathbf{m}_i \in M, \text{s.t.} pr(\mathbf{m}_i) > 0, \mathbf{k}\mathbf{y}_i = \mathbf{m}_i\}, \tag{71}$$

and the expectation of the number of pseudokeys $\overline{K}_P$ is

$$\begin{aligned} \overline{K}_P &= \sum_{(X^{N_K}, Y^{N_K})} \Pr\left(Y^{N_K}, X^{N_K}\right)\left[\left|K\left(Y^{N_K}, X^{N_K}\right)\right| - 1\right] \\ &= \sum_{(X^{N_K}, Y^{N_K})} \Pr\left(Y^{N_K}, X^{N_K}\right)\left|K\left(Y^{N_K}, X^{N_K}\right)\right| - 1, \end{aligned} \tag{72}$$

where $|\mathscr{K}(Y^{N_K}, X^{N_K})|$ represents the number of elements in set $\mathscr{K}(Y^{N_K}, X^{N_K})$.

The application of equation (3) yields

$$\begin{aligned} H\left(K|X^{N_K}, Y^{N_K}\right) &= \sum_{(X^{N_K}, Y^{N_K})} \Pr\left(Y^{N_K}, X^{N_K}\right) H\left(K|Y^{N_K}, X^{N_K}\right) \\ &= \sum_{(X^{N_K}, Y^{N_K})} \Pr\left(Y^{N_K}, X^{N_K}\right) log_2 \left|\mathscr{K}\left(Y^{N_K}, X^{N_K}\right)\right| \leq log_2 \sum_{(X^{N_K}, Y^{N_K})} \Pr\left(Y^{N_K}, X^{N_K}\right)\left|\mathscr{K}\left(Y^{N_K}, X^{N_K}\right)\right| \leq \log_2(\overline{K}_P + 1). \end{aligned} \tag{73}$$

Because of $H(Y^{N_K}|K, M^{N_K}, T^{N_K}, X) = 0$ (it is because the stego object Y can be determined by steganographic key K, data M, distortion function T, and cover object X) and joint entropy $H(M^{N_K}, T^{N_K}, X^{N_K}, K) = N_K(H(X) + H(M) + H(T)) + H(K)$ (it is because the independence of steganographic key K, data M, distortion function T, and cover object X), we can isolate the joint entropy $H(Y^{N_K}, X^{N_K}, M^{N_K}, T^{N_K}, K)$ as

$$\begin{aligned} H\left(Y^{N_K}, X^{N_K}, M^{N_K}, T^{N_K}, K\right) &= H\left(X^{N_K}, M^{N_K}, T^{N_K}, K\right) + H\left(Y^{N_K}|X^{N_K}, M^{N_K}, T^{N_K}, K\right) \\ &= H\left(X^{N_K}, M^{N_K}, T^{N_K}, K\right) = N_K[H(X) + H(M) + H(T)] + H(K). \end{aligned} \tag{74}$$

According to the chain rule of the joint entropy function (equation (2)), we can rearrange the joint entropy $H(Y^{N_K}, X^{N_K}, M^{N_K}, T^{N_K}, K)$ as

$$\begin{aligned} H\left(Y^{N_K}, X^{N_K}, M^{N_K}, T^{N_K}, K\right) &= H\left(X^{N_K}\right) + H\left(Y^{N_K}|X^{N_K}\right) + H\left(K|Y^{N_K}, X^{N_K}\right) + H\left(M^{N_K}|Y^{N_K}, X^{N_K}, K\right) \\ &\quad + H\left(T^{N_K}|M^{N_K}, Y^{N_K}, X^{N_K}, K\right), = N_K H(X) + N_K H(Y|X) + H\left(K|X^{N_K}, Y^{N_K}\right) \\ &\quad + H\left(T^{N_K}|Y^{N_K}, X^{N_K}, M^{N_K}, K\right) \\ &= N_K[(H(X) + H(Y|X) + H(T) - I(T;M,X,Y,K))] + H\left(K|Y^{N_K}, X\right)^{N_K}. \end{aligned} \tag{75}$$

Combining equations (72) and (73), we have

$$\begin{aligned} H\left(K|Y^{N_K}, X^{N_K}\right) = H(K) - N_K[H(Y|X) - H(M) \\ - I(T;M,X,Y,K)]. \end{aligned} \tag{76}$$

Thus,

$$\begin{aligned} \log\left(\overline{K}_p + 1\right) \geq H(K) - N_K(H(Y|X) - H(M)) \\ - I(T;M,X,Y,K)). \end{aligned} \tag{77}$$

Expectation of the number of pseudosteganographic key $\overline{K}_p$ is bounded as

$$\overline{K}_p \geq 2^{H(K)-N_K[H(Y|X)-H(M)-I(T;M,Y,X,K)]} - 1. \quad (78)$$

As a result, the unicity distance N_K is bounded as

$$N_K \geq \frac{H(K|Y)}{H(Y|X) - [H(M) + I(T;Y,X,K)]}, \quad (79)$$

in which $H(K|Y) = \sum_{j=0}^{w_1-1} \log(2^{h-2} - j)$ when the STC parity-check matrix consists of a single submatrix with a width of w_1; $H(K|Y) = \sum_{i=1}^{2} \sum_{j=0}^{w_i-1} \log(2^{h-2} - j)$ when the STC parity-check matrix consists of two submatrices with widths w_1 and w_2.

It can be seen from Theorem 6 that when the relative payload is fixed, the lower bound of the unicity distance of the steganographic key N_K increases as the height h of the submatrix increases; when the number of different submatrices is fixed, the unicity distance of the steganographic key N_K decreases as the relative payload α increases. This is because the larger sizes of submatrices and number of different submatrices mean the more encoding content parameters, that is, the more difficult it is to completely restore the steganographic key. Therefore, the average amount of data required to recover the steganographic key are more. We should choose submatrices with bigger size and a relative payload whose reciprocal is not an integer preferentially. However, the above method will increase the time consumption of generating stego objects.

In this section, the cryptographic secrecy of the STC-based adaptive steganography algorithm is studied from three aspects: the steganographic key equivocation, the message equivocation, and the unicity distance of the steganographic key under the known-cover attack. More specifically, we obtain the upper bound of the amount of steganographic key information and data information leaked from the cover object and stego object, the lower bound of the amount of information an attacker needs to recover the steganographic key, and the quantitative relationship between these theoretical bounds and submatrices, data, and cover object.

5. Discussion and Conclusion

This section mainly uses the results obtained in this manuscript to explain the performance of the data extraction methods proposed in [14–16] and summarizes this manuscript.

5.1. Discussion. The research results of this manuscript show that the cryptographic secrecy of the STC-based adaptive steganography algorithm has a quantitative relationship with the submatrix used by STC under the stego-only attack and the known-cover attack. More specifically, when the number of different submatrices is fixed, the larger size of the submatrix, the stronger the cryptographic secrecy. However, when the height of the submatrix is fixed, the smaller the relative payload, the stronger the cryptographic secrecy is not necessarily. For example, when the height of the submatrix is fixed at 7, the cryptographic secrecy at a relative payload of 0.3 bpp is higher than that at a relative payload of 0.2 bpp. This is because when the height of the submatrix is fixed at 7, there are 49 encoding parameters that need to be restored at a relative payload of 0.3 bpp, while 35 encoding parameters need to be restored at a relative payload of 0.2 bpp. In fact, under different attack conditions, [14–16] all have similar conclusions in different attack methods: the more encoding parameters, the greater the time overhead and the lower the recovery rate. This is because STC are a linear structure, and the more unknowns there are, the more difficult it is to solve. Therefore, when the two parties conduct covert communication, they can select submatrices with greater height and width to enhance the cryptographic secrecy of the covert communication according to actual needs. However, the above method will increase the time consumption of generating the stego object. Thus, we need to make a compromise between cryptographic secrecy and time consumption of generating the stego object.

The research results of Theorem 2 on the steganographic key equivocation in the third section of this manuscript shows that the better the randomness of the embedded data, the smaller the theoretical upper bound of the steganographic key equivocation and the less steganographic key information is obtained from the stego object. This means that, for STC-based adaptive steganography, the randomness of data also has impact on the security of the steganography system. However, the research results of [22] show that even if the data embedded via steganography is unencrypted, as long as the steganography itself has strong cryptographic secrecy, it is still safe in the cryptographic sense. For STC-based adaptive steganography algorithms that use plaintext as data, Luo et al. [15] proposed a data extraction method based on the difference in randomness of the data extracted by correct encoding parameters and the incorrect encoding parameters under the condition of the stego-only attack. When the embedded data is a ciphertext, the random sequence extracted by the incorrect parity-check matrix is indistinguishable from the data extracted by the correct parity-check matrix, which makes the method proposed in [15] invalid. Thus, the sender should encrypt the data when performing covert communication, and the stronger the randomness of the cipher text, the better the cryptographic secrecy of covert communication.

5.2. Conclusion. The STC-based adaptive steganography has become the mainstream steganography technology with strong covert security. However, as the problem of data extraction was put forward, researchers have gradually begun to pay attention to the factors related to the anti-extraction performance of steganography algorithms and what quantitative relationship they have. In the future, the security of STC-based adaptive steganography will gradually get shocked. This manuscript studies the cryptographic secrecy of the STC-based adaptive steganography algorithm from three aspects: steganographic key equivocation, message equivocation, and unicity distance of the steganographic key under the condition of stego-only attack and

known-cover attack. More specifically, based on the special structure of the STC parity-check matrix, we obtain the upper bound of the amount of steganographic key information and data information leaked from the stego object and cover object, the lower bound of the amount of information an attacker needs to recover the steganographic key, and the quantitative relationship between these theoretical bounds and submatrices, data, and cover object. The research results of this manuscript show that the better the randomness of the data and the cover object, the more coding contents parameters of STC, correspondingly the stronger the cryptographic secrecy of the STC-based adaptive steganography algorithm. The research results of this manuscript not only provide precise theoretical guidance for improving the more secure communication based on STC but also provide a theoretical bound of the amount of information required for the attackers to extract data. Next, we will study the data extraction method under the theoretical framework of this manuscript and verify the correctness of the theoretical derivation in this manuscript.

Data Availability

No data were used to support the findings of this study.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

This work was supported by the National Natural Science Foundation of China (nos. U1804263 and 61772549) and Zhongyuan Science and Technology Innovation Leading Talent Project (no. 214200510019).

References

[1] J. Liu, Y. Tian, T. Han, J. Wang, and X. Luo, "Stego key searching for LSB steganography on JPEG decompressed image," *Science China Information Sciences*, vol. 59, no. 3, pp. 56–70, 2016.

[2] A. Ker, P. Bas, R. Bohme, R. Cogranne, and S. Craver, "Moving steganography and steganalysis from the laboratory into the real word," in *Proceedings of the 1st ACM Workshop on Information Hiding and Multimedia Security*, pp. 45–58, Montpellier, France, June 2013.

[3] W. Zhang and S. Li, "Security measurements of steganographic systems," in *Proceedings of the 2nd International Conference on Applied Cryptography and Network Security*, pp. 194–204, Berlin, Germany, June 2004.

[4] S. Jin, F. Liu, C. Yang, Y. Ma, and Y. Liu, "Feature selection of the rich model based on the correlation of feature components," *Security and Communication Networks*, vol. 2021, no. 3, pp. 1–12, 2021.

[5] F. Li, X. Zhang, H. Cheng, and J. Yu, "Digital image steganalysis based on local textural features and double dimensionality reduction," *Security and Communication Networks*, vol. 9, no. 8, pp. 729–736, 2016.

[6] X. Liao, G. Chen, and J. Yin, "Content-adaptive steganalysis for color images," *Security and Communication Networks*, vol. 9, no. 18, pp. 5756–5763, 2016.

[7] C. Yang, X. Luo, J. Liu, and F. Liu, "Extracting hidden messages of MLSB steganography based on optimal stego subset," *Science China Information Sciences*, vol. 61, no. 11, Article ID 109113, 2018.

[8] T. Filler, J. Judas, and J. Fridrich, "Minimizing additive distortion in steganography using syndrome-trellis codes," *IEEE Transactions on Information Forensics and Security*, vol. 6, no. 3, pp. 920–935, 2011.

[9] Y. Zhang, X. Luo, C. Yang, D. Ye, and F. Liu, "A framework of adaptive steganography resisting JPEG compression and detection," *Security and Communication Networks*, vol. 9, no. 15, pp. 2957–2971, 2016.

[10] T. Denemark and J. Fridrich, "Model based steganography with precover," *Electronic Imaging*, vol. 2017, no. 7, pp. 56–66, 2017.

[11] Q. Liu, H. Wu, and X. Zhang, "Adaptive video data hiding with low bit-rate growth based on texture selection and ternary syndrome-trellis coding," *Multimedia Tools and Applications*, vol. 79, no. 43, pp. 32935–32955, 2020.

[12] L. Zhu, X. Luo, C. Yang, Y. Zhang, and F. Liu, "Invariances of jpeg-quantized dct coefficients and their application in robust image steganography," *Signal Processing*, vol. 183, Article ID 108015, 2021.

[13] Y. Zhang, X. Luo, J. Wang, Y. Guo, and F. Liu, "Image robust adaptive steganography adapted to lossy channels in open social networks," *Information Sciences*, vol. 564, pp. 306–326, 2021.

[14] W. Liu, G. Liu, and Y. Dai, ""On recovery of the stego-key in Syndrome-Trellis-Codes," *Information and Control Express Letters*, vol. 8, no. 10, pp. 2901–2906, 2014.

[15] X. Luo, X. Song, X. Li et al., "Steganalysis of HUGO steganography based on parameter recognition of Syndrome-Trellis-Codes," *Multimedia Tools and Applications*, vol. 75, no. 21, pp. 13557–13583, 2016.

[16] J. Gan, J. Liu, X. Luo, C. Yang, and F. Liu, "Reliable steganalysis of HUGO steganography based on partially known plaintext," *Multimedia Tools and Applications*, vol. 77, no. 14, pp. 18007–18027, 2017.

[17] C. Cachin, "An information-theoretic model for steganography," in *Proceedings of the 2nd International Workshop on Information Hiding (IH)*, pp. 306–318, Berlin, Germany, April 1998.

[18] N. Hopper, "Toward a theory of steganography," Technical report, Technical Report CMU-CS-04-157, Carnegie Mellon University, Pittsburth, PA, USA, 2004.

[19] N. Provos and P. Honeyman, "Hide and seek: an introduction to steganography," *IEEE Security & Privacy*, vol. 1, no. 3, pp. 32–44, 2003.

[20] J. Fridrich, M. Goljan, D. Soukal et al., "Searching for the stego key,," in *Proceedings of SPIE-Electronic Imaging, Security, Steganography, and Watermarking of Multimedia Contents VI*, vol. 5306, pp. 70–82, San Jose, CA, USA, June 2004.

[21] J. Fridrich, M. Goljan, D. Soukal, and T. Holotyak, "Forensic steganalysis: determining the stego key in spatial domain steganography," *Proceedings of SPIE-Electronic Imaging, Security, Steganography, and Watermarking of Multimedia Contents VII*, vol. 5681, no. 5, pp. 631–642, 2005.

[22] W. Zhang and S. Li, "Information-theoretic analysis for the difficulty of extracting hidden information," *Wuhan University Journal of Natural Sciences*, vol. 10, no. 1, pp. 315–318, 2005.

[23] J. Fridrich and D. Soukal, "Matrix embedding for large payloads," *IEEE Transactions on Information Forensics and Security*, vol. 1, no. 3, pp. 390–395, 2006.

[24] J. Fridrich, M. Goljan, and D. Soukal, "Wet paper codes with improved embedding efficiency," *IEEE Transactions on Information Forensics and Security*, vol. 1, no. 1, pp. 102–110, 2006.

[25] W. Zhang, X. Zhang, and S. Wang, "Maximizing steganographic embedding efficiency by combining hamming codes and wet paper codes," *Information Hiding* in *Proceedings of the International Workshop on Information Hiding*, vol. 6505, pp. 60–71, Springer, Berlin, Heidelberg, May 2008.

[26] R. Crandall, Some Notes on Steganography, 1998, Steganography Mailing List, http://os.inf.tu-dresden.de/westfeld/crandall.pdf.

[27] P. Regalia, "Cryptographic secrecy of steganographic matrix embedding," *IEEE Transactions on Information Forensics and Security*, vol. 3, no. 14, pp. 786–791, 2008.

[28] J. Chen, J. Liu, W. Zhang, H. Liu, and X. Zhao, "Cryptographic secrecy analysis of matrix embedding," *International Journal of Computational Intelligence Systems*, vol. 6, no. 4, pp. 639–647, 2013.

[29] Y. Zhang, C. Qin, W. Zhang, F. Lu, and X. Luo, "On the fault-tolerant performance for a class of robust image steganography," *Signal Processing*, vol. 146, no. 15, pp. 9–111, 2018.

[30] C. E. Shannon, "Communication theory of secrecy systems," *Bell System Technical Journal*, vol. 28, no. 4, pp. 656–715, 1949.

[31] J. Kodovský and J. Fridrich, "Quantitative steganalysis using rich models," in *Proceedings of SPIE-Electronic Imaging, Media Watermarking, Security and Forensic XV*, vol. 8665, San Francisco, CA, USA, 2013.