Sains Malaysiana 48(12)(2019): 2797–2806
http://dx.doi.org/10.17576/jsm-2019-4812-21

Design of Information Hiding Algorithm for Multi-Link Network Transmission Channel

(Reka Bentuk Maklumat Algoritma Sembunyi untuk Saluran Penghantaran Rangkaian Berbilang Pautan)

SONGYIN FU & RANGDING WANG*

ABSTRACT

Traditional channel information hiding algorithms based on m-sequence for multi-link network transmission, which apply m-sequence to channel coding information hiding system, do not analyze the upper limit of hiding capacity of multi-link network transmission channel system, and do not consider the hidden danger of overlapping secret information when embedding secret information is too large. It has the defects of low efficiency, poor accuracy and large storage cost. This paper designs an information hiding algorithm for multi-link network transmission channel based on secondary positioning, it uses RS code M public key cryptosystem to pre-process secret information and improve the security of information; calculates the upper limit of hiding capacity of multi-link network transmission channel system through information hiding capacity analysis model, and determines whether the hiding capacity exceeds the secret information. Secondary location and cyclic shift mechanism are introduced to improve the randomness of location selection and avoid overlapping of secret information. The experimental results show that the proposed algorithm has a great advantage in memory cost. When the channel SNR is 0 dB and 8 dB, the normalization coefficients are 0.87 and 1.04, respectively. This shows that the algorithm has a high accuracy in extracting secret information. The average time spent on hiding information is 2.04 s, indicating that the algorithm has high information hiding rate and storage efficiency.

Keywords: Coding channel; information hiding; multi-link; network transmission channel; preprocessing; secondary embedding

ABSTRAK

Saluran tradisi algoritma penyembunyian maklumat berdasarkan jujukan-m untuk penyampaian rangkaian berbilang pautan yang menggunakan jujukan-m untuk menyalurkan maklumat pengekodan sistem sembunyi tidak menganalisis had atas kapasiti sembunyi sistem saluran penghantaran rangkaian berbilang pautan dan tidak mempertimbangkan bahaya tersembunyi akibat pertindihan maklumat rahsia apabila pembenaman maklumat rahsia adalah terlalu besar. Ia mempunyai kecacatan kecekapan yang rendah, ketepatan yang lemah dan kos storan yang tinggi. Kertas ini mereka bentuk algoritma penyembunyikan maklumat untuk penghantaran saluran rangkaian berbilang pautan berdasarkan kedudukan sekunder, ia menggunakan sistem kripto kunci awam RS kod M untuk prapemprosesan maklumat rahsia dan meningkatkan keselamatan maklumat; menghitung had atas kapasiti sembunyi sistem penghantaran saluran rangkaian berbilang pautan melalui model analisis kapasiti penyembunyian maklumat dan menentukan sama ada kapasiti persembunyian melebihi maklumat rahsia. Lokasi sekunder dan mekanisme peralihan kitaran diperkenalkan untuk menambahbaik pemilihan lokasi secara rawak dan mengelakkan pertindihan maklumat rahsia. Hasil uji kaji menunjukkan bahawa algoritma yang dicadangkan mempunyai kelebihan yang besar dalam kos ingatan. Apabila saluran SNR adalah 0 dB dan 8 dB, pekali penormalan masing-masing adalah 0.87 dan 1.04. Ini menunjukkan bahawa algoritma mempunyai ketepatan yang tinggi dalam mengekstrak maklumat rahsia. Masa purata yang digunakan untuk menyembunyikan maklumat adalah 2.04 s, menunjukkan bahawa algoritma ini mempunyai kadar penyembunyian maklumat yang tinggi dan kecekapan penyimpanan.

Kata kunci: Berbilang pautan; pembenaman sekunder; penyembunyian maklumat; prapemprosesan; saluran pengekodan; saluran penghantaran rangkaian

INTRODUCTION

Information hiding is a new information security technology, with strong information security and information security (Palanimuthu & Muthial 2017), has been developed rapidly in recent years. At present, information hiding research is mostly focused on text, image, audio and video carriers, but when using these digital media as a carrier to hide data, it will inevitably change the number of some bits of source data (Xie et al. 2016). However, there is little research on the key issues of information hiding in multi-link network transmission channels, especially in coded transmission channels. The encoding transmission channel here refers to the channel using channel coding technology to achieve reliable transmission. The channel coding technology used includes RS coding, BCH coding, convolution coding and LDPC coding.

Channel coding is a technology to improve the reliability of data transmission in multi-link networks. Channel coding information hiding technology uses the phenomenon of channel noise to embed secret information as artificial noise within the range of error correction ability of channel coding (Gong et al. 2017). The use of channel coded codewords as embedded carriers effectively overcomes the problems brought about by digital media as carriers. On the one hand, embedding secret information into channel coding in multi-link networks will not affect the structure and statistical characteristics of the original information data, and certainly will not change the decoded data visually or audibly, as long as the overall effect of embedded secret information (artificial noise) and channel noise is not guaranteed. If the error correction ability of channel coding is beyond the range, the original information can be correctly restored after channel decoding. On the other hand, channel coding technology is more widely used in modern communications, both satellite communications and short-wave communications, have been widely used in channel coding technology, which makes the channel coding as a carrier for information hiding feasible.

At present, there are two main aspects in the research of channel coding related multi-link network transmission information hiding technology: Using RS, BCH and other error-correcting coding technology in the pre-embedding multi-link network secret information processing or carrier information processing to improve the performance of hiding and extracting (Zhang et al. 2016); and the technology of information hiding in redundant link of multi-link network coding channel is used.

Previous studies have shown that when data is transmitted over a multi-link network channel, interference in the channel may cause random errors in the received information. Error correction coding technology can improve the occurrence of such errors and provide a certain amount of coding error correction space (Zhao & Chen 2015). This phenomenon provides a basis for the realization of information hiding on coding channels. In principle, as long as the sum of permutation error codes and channel interference errors caused by secret information hiding in multi-link networks is less than the error-correcting ability of channel coding, the secret information can be hidden as noise into the channel-coded data stream, which will not change the audio-visual performance of the decoded secret data, and let alone the audio-visual performance. It will change the statistical characteristics of the original carrier (Wang et al. 2018). With the enhancement of channel coding error correction capability, the non-detectability and security of secret information in multi-link networks will be improved, and the hidden capacity of multi-link networks will be increased (Gulbahar 2017).

The traditional channel information hiding algorithm for multi-link network transmission based on m-sequence applies m-sequence to the channel coding information hiding system (Gao et al. 2017). The main method is to use random m-sequence to deal with the secret information itself and the embedded position disturbance. It does not analyze the capacity of the multi-link network transmission channel system. Considering the hidden danger of overlapping secret information when the embedded secret information is too large, it has the disadvantages of slow speed, low accuracy and large storage cost. Aiming at the shortcomings of traditional algorithms, this paper proposes a coding channel information hiding algorithm based on secondary localization. The upper limit of system hiding capacity is fully considered before the secret information is embedded, and the mechanism of secondary localization and cyclic shift is introduced in the process of selecting the embedded position, which can avoid the error of information hiding and at the same time avoid the error of information hiding. It can improve the randomness of embedding location selection and avoid the risk of mutual covert information.

Information Hiding Algorithm For Multi-Link Network Transmission Channel Based on Secondary Location

PREPROCESSING OF SECRET INFORMATION

Secret information security is a key problem to be solved in multi-link network transmission channel system. Therefore, it is necessary to pre-process the secret information before embedding it into the carrier. Li and Chen (2015) proposed the pre-processing steps of scrambling code and channel coding: Add the secret information to the pseudo-random sequence. By means of scrambling and channel coding, the randomness and reliability of secret information in multi-link network transmission channel can be improved, and it can be changed into approximate random digital sequence. For the above preconditioning methods, if the amount of secret information is large enough to meet the conditions of blind analysis of corresponding channel coding codes and scrambling codes, then the secret information is unsafe. In order to further improve the security of secret information in multi-link network transmission channel, a new scheme of secret information preprocessing is proposed in this paper: RS code M public key cryptosystem is used in the process of secret information coding in multi-link network transmission channel.

Assume that n, k, and t represent the code length, information length, and error correction capability, respectively. The private key consists of three parts: They are the $k \times n$ order generation matrix G, the RS code (2^m) on the error finite field GF , and the randomly selected $k \times k$ non-singular matrix S. P is a $n \times n$-order permutation matrix, and the triple (S^{-1}, G, P^{-1}) is a private key. The so-called permutation matrix means that each row and column has only one "1" and the rest is " 0". Its function is to multiply any set of data and only change the order of the elements in the original data (Xu et al. 2015). The public key is the error-correcting ability t of the $k \times n$ matrix G^* and the code. The G^* is obtained in advance from the formula $G^* = SGP$. Encryption transformation: Random selection of a n dimension vector $u = (u_{n-1}, u_{n-2}, \mathrm{L}, u_0)$ on $\mathrm{GF}(2^m)$, its

weight is not greater than t, that is, $W(u) = t' \le t$, then the operation $c = mG^* + u$ can be sent ciphertext c.

The decryption transformation is calculated first.

$$cP^{-1} = (mG^* + u)P^{-1} = (mSGP)P^{-1} + uP^{-1}$$

$$= mSG + uP^{-1} = mSG + u' \quad (1)$$

Because P is a permutation matrix, P^{-1} is also a permutation matrix, u' is the product of u and P^{-1}, that is, u' is a permutation of u, therefore, u' weight also meets $W(u') = t' \le t$, that is, cP^{-1} consists of two parts, one is the combination of the information group mS of m and the generation matrix G multiplication generated (n, k) code $v = m'G = mSG$. The other part is the permutation u of random vector u' added randomly., because of $W(u') = t' \le t$, within the error-correcting ability of the code, gets the correct code $v = mSG$ and the linear combination mS of the information group after error-correcting decoding, then multiplies mS with S^{-1} to get the plaintext $m = (mS)S^{-1}$. It should be noted that it is necessary to add a random vector u to the encryption process. Otherwise, the interceptor can solve the plaintext mm according to mG^* and the intercepted ciphertext.

INFORMATION HIDING CAPACITY ANALYSIS MODEL

In order to improve the security and robustness of the multi-link network transmission channel system, the transmitter preprocesses the secret information such as scrambling, encrypting and error-correcting coding. In order to prevent the size of the secret information from exceeding the capacity of the multi-link network transmission channel system and destroying the non-detectability of the system, the information hiding capacity analysis model is introduced. Considering the error-correcting ability of channel coding in multi-link networks, the total error caused by the replacement of hidden information and channel interference should be guaranteed to be within the error-correcting range of channel coding before hiding information. Only in this case can the receiver receive the source information without distortion and extract it without error (Che et al. 2015). The capacity analysis of information hiding based on coded channel is based on the size of secret information. An example of a channel coded packet (shown in Figure 1) is given to illustrate the information hiding capacity analysis process of the coded channel.

As shown in Figure 1, the channel coding parameter is (n, k, t), and the bit error rate caused by channel interference is p_b. In addition, $(m_1, m_2, \mathrm{L}, m_M)$ denotes secret information, k denotes encoded input length, n denotes encoded output length, and n denotes the number of error corrections in a single channel encoded packet. The secret information is embedded into the corresponding position of the channel coding packet, and the worst case is that the secret information is opposite to the source information in the corresponding position. That is to say, the secret information is interference to the encoded data stream (Huang 2016), and the number of bit errors caused by the secret information is M. The camouflage data stream embedded with secret information is transmitted through the channel, which will cause certain error code due to channel noise and other interference. As shown in Figure 2, the sequence of secret information has already been

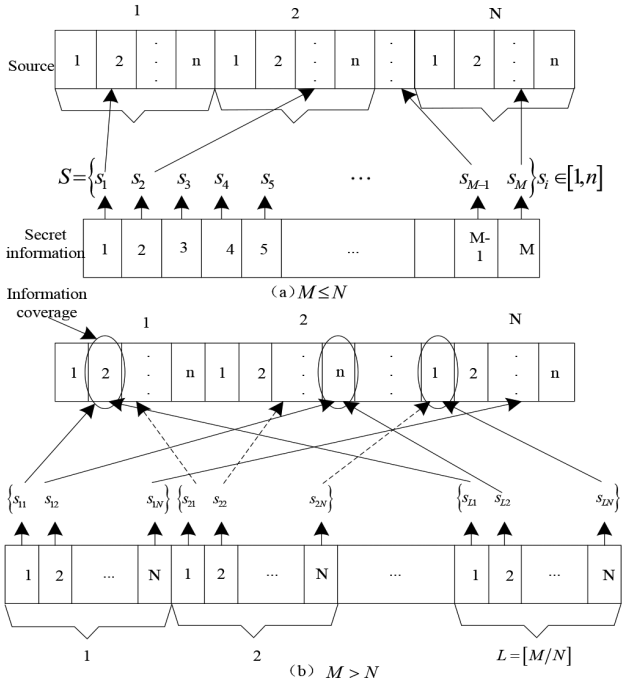

FIGURE 1. Secret information coverage process

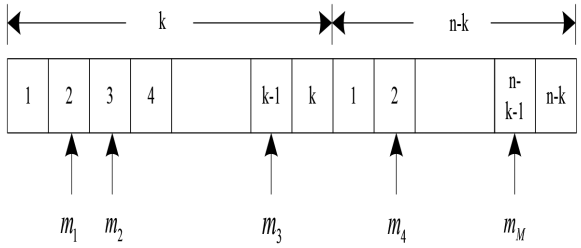

FIGURE 2. Analysis of information hiding capacity in coded channel

included in the data stream to be transmitted with length n, so the bit error caused by secret information cannot be calculated repeatedly, that is, the bit error caused by channel interference is $(n - M)p_b$ after transmission through the channel. To sum up, the total error of secret information and channel interference is $M + (n - M)p_b$.

Suppose the parameters of the multi-link network transmission channel system are set as follows:

C_0: The length of the source data stream; C: The length of the source data after channel coding; $m_0 = (m_{01}, m_{02}, \mathrm{L}, m_{0M_0})$: Secret information stream; $m = (m_1, m_2, \mathrm{L}, m_M)$: Preprocessed secret information; $E(C, m, K)$: $M + (CP_b - MP_b) \le \frac{C}{n_1} t_1$ Secret information embedding algorithm; and $D(C', K)$: Secret information extraction algorithm.

Among them, M_0 is the length of secret information; M is the length of pre-processed secret information; K is the key agreed by both parties, which is used to generate pseudo-random sequence to determine the embedded location of secret information; and p_b is the bit error rate of channel. If the channel coding type is block code and the channel coding parameter is (n_1, k_1, t_1), the capacity of information hiding based on block channel coding is as follows:

$$M + (CP_b - MP_b) \le \frac{C}{n_1} t_1 \tag{2}$$

$$M = \frac{\frac{C}{n_1} t_1 - CP_b}{1 - P_b} \tag{3}$$

$$M_{\max} = \left\lfloor \frac{C_0}{k_1} \right\rfloor \frac{t_1 - n_1 P_b}{1 - P_b} \tag{4}$$

If the preprocessing method does not change the size of secret information, the capacity of information hiding based on block channel coding is $M_{\max}$; if the secret information is preprocessed by error-correcting coding (Wang et al. 2015) and the error-correcting coding parameter is (n_2, k_2, t_2), the capacity of information hiding based on block channel coding for multi-link network transmission channel is:

$$M_{0\max} = \left\lfloor \frac{C_0}{k_1} \right\rfloor \frac{t_1 - n_1 P_b}{1 - P_b} \frac{k_2}{n_2} \tag{5}$$

If the channel coding type is convolutional code (Galdino et al. 2016), let the channel coding parameter as (n_1, k_1, t_1), where L denotes the length of coding constraint, and its value is generally $L = (t_1 + 1)n_1$, indicating that the current code group is related to the previous code group (Kazemi & Tajer 2018), and t_1 denotes the number of correctable errors in the length of coding constraint, then the multi-link network transmission based on convolutional channel coding is carried out. The capacity of channel information hiding is:

$$M + (CP_b - MP_b) \le \frac{C}{L} t_1 \tag{6}$$

$$M \le \frac{\frac{C}{L} t_1 - CP_b}{1 - P_b} \tag{7}$$

$$M_{\max} = \left\lfloor \frac{C_0}{k_1} \right\rfloor n_1 \frac{\frac{t_1}{L} - P_b}{1 - P_b} \tag{8}$$

Similarly, the capacity of information hiding based on convolutional channel coding is $M_{\max}$ if the size of secret information in the multi-link network transmission channel is not changed by the pre-processing method; if the secret information is pre-processed by error-correcting coding method and the error-correcting coding parameter is (n_2, k_2, t_2), the multi-link network transmission channel based on convolutional channel coding is proposed. The capacity of information hiding is:

$$M_{0\max} = \left\lfloor \frac{C_0}{k_1} \right\rfloor n_1 \frac{\frac{t_1}{L} - P_b}{1 - P_b} \frac{k_2}{n_2} \tag{9}$$

SECONDARY LOCATION EMBEDDING MECHANISM

In order to improve the randomness of channel information embedding location selection in multi-link networks, a secondary location embedding mechanism is introduced. The secondary positioning and embedding mechanism is shown in Figure 3.

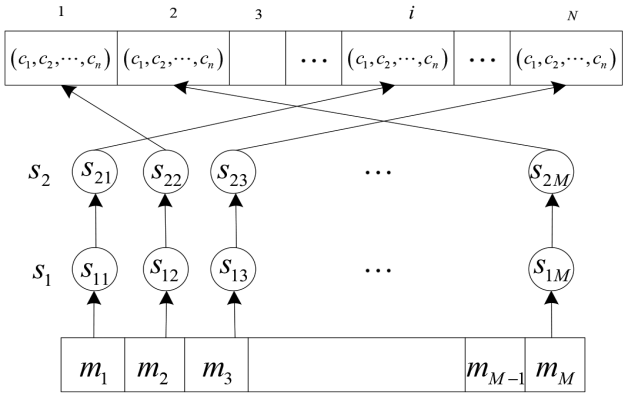

FIGURE 3. Schematic diagram of two level positioning and embedding mechanism

In Figure 3, assuming that the coding output length of the transmission channel in a multi-link network is n, the number of packets is N, the secret information length is M, and $M \le N$, the secondary localization algorithm can be expressed as follows: first, the packet selection sequence S_1 is generated according to the secret information length in the transmission channel of a multi-link network, and its value is $S_1 = (s_{11}, s_{12}, \mathrm{L}, s_{1M})$, that is, the element value in S_1 is an integer. Then the pseudo-random sequence S_2 is generated according to the key K and the secret information length mm, whose value $S_2 = (s_{21}, s_{22}, \mathrm{L}, s_{2n})$, $1 \le s_{2i} \le n$; finally, for the i bit secret information, the embedded packet location is selected according to the s_{1i} value in S_1, and the specific location in the packet is determined according to the S_{2i} value in S_2. Comparing with the traditional algorithm, which embeds the i bit secret information into the s_i bit of the i group carrier data according to the random number s_i, the embedding position of each bit secret information in this algorithm is determined by the sequence S_1 and sequence S_2 (Wu et al. 2017), therefore, the multi-chain is improved to a certain extent. The randomness of location selection of network transmission channel information.

However, when $M > N$ is used, the problem of information coverage appears. In the algorithm, in order to ensure that the hidden information does not appear overlay phenomenon, the selection of embedding location is improved.

Firstly, the length of hidden information and the number of channel coded packets are judged: if the length of hidden information is not larger than the number of packets, then the embedding position is selected according to the secondary positioning mechanism. If the length of hidden information is larger than the number of packets, then $S_1 = randperm(1, N)$, and the secret information needs to be grouped according to the number of packets, the number of packets is $Packets\ \lceil M/N \rceil$. The first group is embedded according to the method of $M \le N$. After the embedding is completed, the S_2 value is added with a modular n to achieve cyclic shift, and the position selection sequence (Yue et al. 2015) of the next set of secret information is obtained. After n–1 sub-shifting, n sequences with different location selections can be obtained, which can be used as position selections of n group secret information at most. The number of shifts is identified by variable *ncount*, and so on, until the secret information is embedded or $ncount = n$ ends. Generally speaking, if the length of the secret information meets the requirement of the system hiding capacity, the secret information can be fully embedded in the channel (Wu et al. 2015) before the condition $ncount = n$ is satisfied.

In summary, compared with the traditional algorithm, the proposed algorithm fully considers the upper limit of information hiding capacity in multi-link network before embedding secret information, and avoids the risk of secret channel exposure in multi-link network caused by excessive hiding capacity (Calabuig et al. 2015). Moreover, when the secret information is large, the algorithm introduces secondary location and cyclic shift mechanism in the process of embedded location selection, which not only improves the randomness of embedded location selection, but also avoids the risk of secret information overlay (Gao & Wang 2017; Monte 2018; Peng et al. 2017; Regees 2017; Ünsal & Knopp 2015). The specific process is shown in Figure 4.

RESULTS

In order to verify the validity of the proposed channel information hiding algorithm for multi-link networks based on secondary positioning, the system RS (255, 215) code is used to encode the source. The code is generated by the primitive polynomial $f(x) = x^8 + x^7 + x^2 + x + 1$ in the GF (2^8) domain, and the error of 20 consecutive symbols can be corrected at most. There are 160 bits of error in succession. The secret information is encoded by BCH (63, 51) code, which can correct 2-bit error. The source and the secret information are 257k byte BMP images and 13K byte JPEG images respectively. We start embedding hidden data from seventh code groups of the secret carrier, the random sequence S2 with an average distribution in (215, 216, ..., 255) controls the embedding bits, the random sequence S3 with an average distribution in (12, 13, ..., 16) controls embedding quantity. The source image is shown in Figure 5(a), and stealth information is shown in Figure 6(a). When

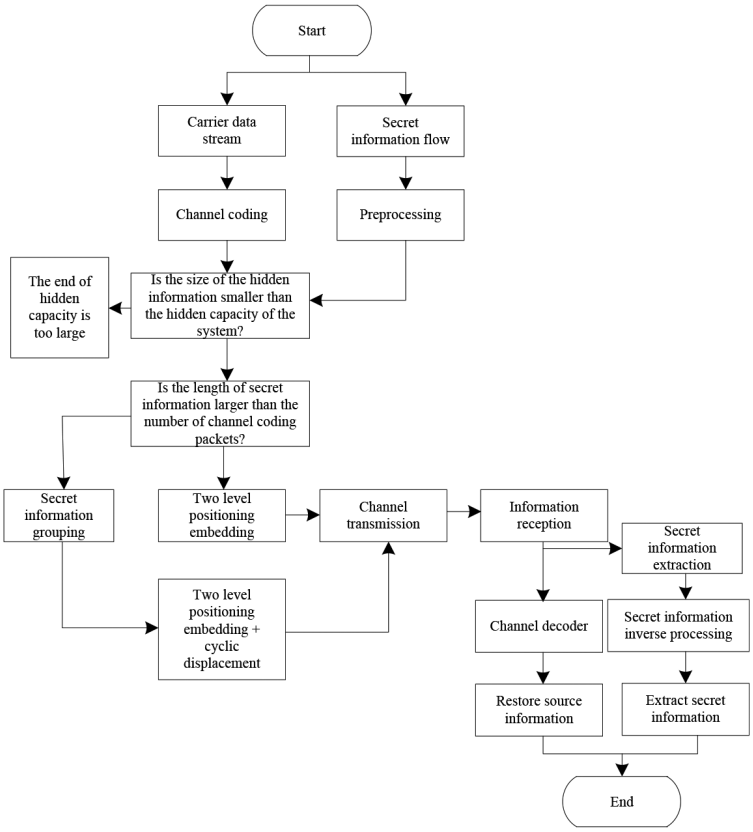

FIGURE 4. Flow chart of information hiding algorithm for multi-link undisturbed network transmission channel

the channel BER is less than or equal to 10^{-2}, there is no effect on the decoded source. Figure 5(d) is the original image received without decoding at this time; when the channel BER reaches 2%, the decoded carrier source image is shown in Figure 5(b), and the recovered covert information is shown in Figure 6(b); when the channel BER reaches 5%, the decoded carrier source image is shown in Figure 5(b). The carrier source image is shown in Figure 5(c), and the image of the stealth information cannot be recovered at this time.

As shown in Figures 5 and 6, when the embedding rate of the hidden information is 4.7%-6.2%, and the channel error rate is below 10^{-2}, the channel noise has no effect on the decoded carrier source image and the hidden information; when the channel error rate is equal to 2%, the errors in some code-words cannot be corrected, and the decoded carrier source image can be seen dimly. When the channel error rate is equal to 5%, all the errors in the code-word cannot be corrected. The snowflake-like noise in the decoded carrier source image is more obvious because the channel noise destroys some coding parameters in the JPEG image data and cannot recover the hidden image. It is found

(a) Source image (b) Image with error rate of 2%

(c) Image with error rate of 5% (d) Original image received directly

FIGURE 5. Related images of source images

(a) Secret information (b) Secret information of recovery

FIGURE 6. Related images of secret information

that if the bit error rate is larger, the carrier source image has obvious snowflake noise. Therefore, in the experiments, when the channel BER is 10^{-2}, the weight of the embedding rate is 6.2%. If the embedding rate exceeds this weight, the carrier source image will be distorted. Experimental results show that the proposed algorithm can effectively hide channel information in multi-link networks.

Experiments were carried out to verify the storage cost performance of the algorithm, and compare the algorithm and the traditional algorithm. It is assumed that the secret information does not exceed the maximum hiding capacity of a multi-link network transmission system, and the ratio of the length of the information to the number of channel coded packets $R(R \geq 1)$ is assumed. The ratio indicates that the information embedded in each channel coding packet is R_{bit}. If only 1-bit information is embedded in each packet by one embedding operation, the ratio R indicates that R embedding operations are needed to hide the information completely, and then the overhead of the two algorithms on key distribution and pseudo-random sequence storage is shown in Table 1.

TABLE 1. Storage overhead of different algorithms

Algorithm	Storage overhead	
	Key number	Pseudorandom sequence number
Algorithm in this paper	1	2
Traditional algorithm	R	R

As can be seen from Table 1, the storage space of the traditional algorithm increases with the increase of R. Only in the case of $R = 1$, the performance of the traditional algorithm is slightly better than that of the algorithm in this paper. $R = 1$ indicates that the size of secret information is not larger than the number of channel coded packets, that is, as many as 1-bit secret information is embedded in each channel coded packet. This situation is extremely strict for the size of secret information. When $R \geq 2$, the storage space of the algorithm is much smaller than the traditional algorithm. Generally, the multi-link network transmission channel system should ensure a certain hiding capacity, and without affecting the invisibility of the system, it is best to hide as much information as possible. The development of multi-link network transmission channel system is sure to achieve the security hiding of large capacity information. Therefore, for large capacity multi-link network transmission channel system, the proposed algorithm has a greater advantage in storage overhead.

Normalized coefficient (NC) value is usually used to describe the similarity between the original secret information and the extracted secret information in multi-link network transmission channel system. The larger NC value is, the more accurate the extracted secret information is, and the better the robustness of the system is. In order to verify the robustness of the proposed algorithm, the NC values of the same secret information under different channel SNR are compared by using the proposed algorithm and the traditional algorithm, respectively. The results are described in Figure 7.

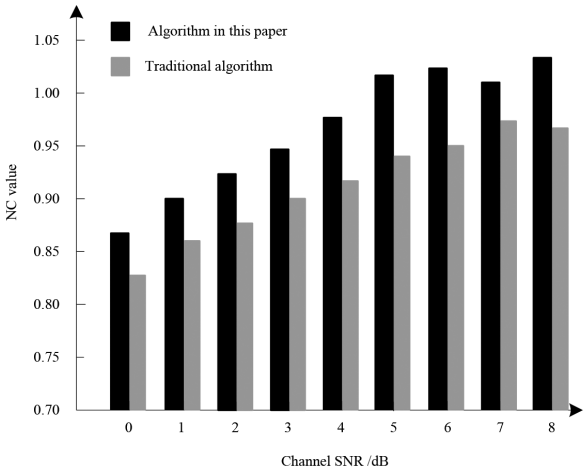

FIGURE 7. Normalization coefficient of secret information obtained by different algorithms

Analysis of Figure 7 shows that when the channel SNR is 0 dB, the NC value of the proposed algorithm is 0.87 and the NC value of the traditional algorithm is 0.83; when the channel SNR is 8 dB, the NC value of the proposed algorithm is 1.04 and the NC value of the traditional algorithm is 0.96. The NC value of secret information obtained by the proposed algorithm is obviously higher than that by the traditional algorithm, especially when the channel conditions are not ideal. However, the improvement of NC value is not infinite. When the channel conditions are good and the secret information can be extracted completely without error, the NC value tends to be stable. Experimental results show that the proposed algorithm has high accuracy for channel information hiding in multi-link networks.

In order to test the speed of information hiding in multi-link network transmission channel, five algorithms are used to hide information in the same experimental environment, such as this algorithm, M-sequence-based multi-link network transmission channel information hiding algorithm and LDPC-coded channel information hiding algorithm. The time spent on the law is shown in Table 2.

Table 2 shows that in the same multi-link network transmission environment, the average time required for information hiding using this algorithm is 2.04 s; the average time required for information hiding using M-sequence based multi-link network transmission channel information hiding algorithm is 4.96 s; and the information hiding algorithm based on LDPC coding channel is 5.96 s. The other two algorithms require 4.05

TABLE 2. The time required for different algorithms to hide information

Number of times / times	Information hiding algorithm for multi- link network transmission channel based on m sequence/s	Information hiding algorithm based on error correcting coding/s	Information hiding algorithm based on LDPC coding channel/s	Channel information hiding algorithm based on RS coding/s	Algorithm in this paper/s
1	4.63	3.77	6.27	4.39	1.84
2	4.54	3.96	5.46	4.74	2.11
3	4.67	4.21	6.13	4.81	2.06
4	4.89	4.05	6.02	4.58	1.95
5	5.06	3.83	5.68	4.76	2.30
6	5.17	3.97	5.88	3.99	2.61
7	4.93	4.02	5.52	5.02	2.12
8	5.38	4.36	6.04	5.10	1.84
9	5.22	4.41	6.37	4.84	1.57
10	5.09	3.92	6.21	4.97	2.03
Average value	4.96	4.05	5.96	4.72	2.04

s and 4.72 s, respectively. At the same time, compared with other algorithms, the time required for this algorithm is relatively mild. Experimental results show that the proposed algorithm can hide channel information in multi-link networks at a faster speed.

In order to verify the advantages of the proposed algorithm, the performance of the proposed algorithm and the other four algorithms, including the traditional m-sequence based channel information hiding algorithm for multi-link network transmission, are compared and analyzed in three aspects: prevention mechanism, location method and cyclic displacement (Table 3).

Compared with other four algorithms, this algorithm constructs a capacity analysis model in the prevention mechanism, and applies this model in the specific operation process. In the positioning method, this algorithm uses secondary positioning, which makes the positioning results more accurate; in the cyclic displacement, it is the only use of cyclic displacement and prevents covert information related coverage. Experimental results show that the proposed algorithm has a high advantage in hiding channel information of multi-link networks.

DISCUSSION

The similarity between the original secret information and the extracted secret information, that is, the normalized coefficient (NC) value, is the most powerful proof of the effect of information hiding. The experimental results show that the NC value of the proposed algorithm is improved to varying degrees compared with the traditional algorithm under different noise-saving conditions, which shows that the accuracy of this paper is higher and the robustness is better. The main reason is that the RS code M public key cryptosystem is introduced into the algorithm to preprocess the secret information in the multi-link network transmission channel system, which enhances the error correction ability of the code.

The primary goal of channel information hiding is to transmit secret information smoothly. Generally, the secret information that needs to be hidden has high value. Therefore, the speed of transmitting secret information is considered as an important factor in designing channel information hiding algorithm. Compared with the traditional algorithm, the average time of information hiding is doubled in this paper. The main reason is

TABLE 3. Analysis of advantages of different algorithms

Algorithm	Prevention mechanism	Positioning method	Cyclic displacement
Information hiding algorithm for multi-link network transmission channel based on m sequence	No	Wavelet domain embedding	No
Information hiding algorithm based on error correcting coding	A capacity analysis model is proposed	No	No
Information hiding algorithm based on LDPC coding channel	Building capacity analysis model	Single location	No
Channel information hiding algorithm based on RS coding	No	Single location	No
Algorithm in this paper	Build the capacity analysis model and apply it to the specific algorithm	Two level positioning, more flexible and accurate	With cyclic displacement mechanism to prevent covert information related coverage

that the secondary location embedding mechanism is adopted in this algorithm. The ratio of the length of the information to the number of channel coded packets is described by $R(R \geq 1)$. The traditional algorithm needs R embedding operation to embed the information. Secret information is completely hidden, and the algorithm in this paper only needs one key and two pseudo-random sequences to complete the embedding operation. In the multi-link network transmission channel, the security of large-capacity information hiding, not only has a greater advantage in storage overhead, but also saves the embedding operation time, and improves the speed of information hiding.

Conclusion

Aiming at the problem that the capacity of multi-link network transmission channel system is not analyzed in the traditional algorithm, and the hidden danger of overlapping secret information when embedding secret information is too large, a multi-link network transmission channel information hiding algorithm based on secondary positioning is designed. RS code M public key cryptosystem is used to preprocess secret information. To realize the pretreatment of secret information, the upper limit of system hiding capacity is analyzed and considered before the embedding of secret information. Secondary location and cyclic shift mechanism are introduced in the embedding location selection process. Experiments show that the proposed algorithm can hide channel information effectively in multi-link networks, and has a great advantage in storage overhead. When the channel SNR is 0 dB and 8 dB, the NC value of the proposed algorithm is increased by 0.04 and 0.08 respectively compared with the traditional algorithm. The average hiding time of the proposed algorithm is improved by 1 fold compared with other algorithms. This algorithm can quickly and accurately hide multi-link network transmission channel information. With the demand of large capacity information hiding and the development of channel coding technology, the coding channel information hiding technology based on secondary positioning will be widely developed and applied.

Acknowledgements

The study was supported by the National Natural Science Foundation of China ('Passive Forensic for Digital Speech Based on Deep Learning' Grant No. 61672302, 'The Study of Secure Steganography and Its Countermeasure Technique Applicable to a Variety of Digital Medias' Grant No. U1736215), Ningbo University Fund (Research on the key technology of collision resistance on MAC layer in WSN network Grant No. XKXL1509) and K.C. Wong Magna Fund in Ningbo University.

References

Calabuig, D., Gohary, R.H. & Yanikomeroglu, H. 2015. Optimum transmission through the multiple-antenna gaussian multiple access channel. *IEEE Transactions on Information Theory* 62(1): 230-243.

Che, Y., Xu, J., Duan, L. & Zhang, R. 2015. Multiantenna wireless powered communication with cochannel energy and information transfer. *IEEE Communications Letters* 19(12): 2266-2269.

Galdino, L., Tan, M., Alvarado, A., Lavery, D., Rosa, P., Maher, R., Ania-Castañón, J.D., Harper, P., Makovejs, S., Thomsen, B.C. & P. Bayve. 2016. Amplification schemes and multi-channel dbp for unrepeatered transmission. *Journal of Lightwave Technology* 34(9): 2221-2227.

Gao, W. & Wang, W.F. 2017. The fifth geometric-arithmetic index of bridge graph and carbon nanocones. *Journal of Difference Equations and Applications* 23(1-2SI): 100-109.

Gao, Y., Wen, A., Zhang, W., Wang, Y. & Zhang, H. 2017. Photonic microwave and mm-wave mixer for multi-channel fiber transmission. *Journal of Lightwave Technology* 35(9): 1566-1574.

Gong, S., Xing, C., Yang, N., Wu, Y.C. & Fei, Z. 2017. Energy efficient transmission in multi-user MIMO relay channels with perfect and imperfect channel state information. *IEEE Transactions on Wireless Communications* 16(6): 3885-3898.

Gulbahar, B. 2017. A communication theoretical analysis of multiple-access channel capacity in magneto-inductive wireless networks. *IEEE Transactions on Communications* 65(6): 2594-2607.

Huang, M.C. 2016. Novel time-frequency cross methods to resolve EMI issues. *Journal of Power Supply* 14(5): 167-171.

Kazemi, S. & Tajer, A. 2018. Multiaccess communication *via* a broadcast approach adapted to the multiuser channel. *IEEE Transactions on Communications* 66(8): 3341-3353.

Li, D.S. & Chen, Z.G. 2015. A new method to prevent trojan-in node based on inner secure tunnel. *Journal of China Academy of Electronics and Information Technology* 10(4): 379-382.

Monte, L. 2018. Nonlinear Leslie models for the assessment of the effects of stressors on the development of wild populations: Reviewing of the basic properties. *Journal of Interdisciplinary Mathematics* 21(1): 83-109.

Palanimuthu, S.J. & Muthial, C. 2017. An enhanced multi-channel bacterial foraging optimization algorithm for MIMO communication system. *International Journal of Electronics* 104(4): 608-623.

Peng, W., Ge, S., Ebadi, A.G., Hisoriev, H. & Esfahani, M.J. 2017. Syngas production by catalytic co-gasification of coal-biomass blends in a circulating fluidized bed gasifier. *Journal of Cleaner Production* 168: 1513-1517.

Regees, M. 2017. Super edge trimagic total labeling of some star type graphs. *Journal of Discrete Mathematical Sciences and Cryptography* 20(3): 747-754.

Ünsal, A. & Knopp, R. 2015. Distributed sensing and transmission of sporadic random samples over a multiple-access channel. *IEEE Transactions on Communications* 63(10): 3813-3828.

Wang, D., Li, Z., Zhang, N., Wu, H. & Shen, X. 2018. Channel states classification in cognitive small cell networks with multiple transmission powers. *IEEE Transactions on Vehicular Technology* 67(7): 6023-6036.

Wang, D., Toni, L., Cosman, P.C. & Milstein, L.B. 2015. Resource allocation and performance analysis for multiuser video transmission over doubly selective channels. *IEEE Transactions on Wireless Communications* 14(4): 1954-1966.

Wu, H., Tao, X., Han, Z., Li, N. & Xu, J. 2017. Secure transmission in MISOME wiretap channel with multiple assisting jammers: Maximum secrecy rate and optimal power allocation. *IEEE Transactions on Communication* 65(2): 775-789.

Wu, S., Wei, S., Wang, Y., Vaidyanathan, R. & Yuan, J. 2015. Partition information and its transmission over boolean multi-access channels. *IEEE Transactions on Information Theory* 61(2): 1010-1027.

Xie, K., Wang, X., Liu, X., Wen, J. & Cao, J. 2016. Interference-aware cooperative communication in multi-radio multi-channel wireless networks. *IEEE Transactions on Computers* 65(5):1528-1542.

Xu, Y., Wu, Q., Wang, J., Shen, L.P. & Anpalgan, A. 2015. Robust multiuser sequential channel sensing and access in dynamic cognitive radio networks: Potential games and stochastic learning. *IEEE Transactions on Vehicular Technology* 64(8): 3594-3607.

Yue, X., Zhou, C., Gan, W.D. & Minglong, Z. 2015. Research and simulation of data hiding algorithm in military image encryption communication. *Computer Simulation* 32(3): 238-241.

Zhang, L., Zhu, Y. & Zheng, W.X. 2016. State estimation of discrete-time switched neural networks with multiple communication channels. *IEEE Transactions on Cybernetics* 99: 1-13.

Zhao, L.J. & Chen, Y.J. 2015. Research on digital image scrambling technology in information hiding. *Automation and Instrumentation* 6: 135-137.

Faculty of Electrical Engineering and Computer Science
Ningbo University
Ningbo, 315211
China

*Corresponding author; email: wangrangding@nbu.edu.cn

Received: 21 February 2019
Accepted: 23 December 2019