Enhancing Physical Layer Security via Information Hiding and Chaotic Frequency-Hopping Signal

MingQuan Fan (mqfan_sc@163.com)
Southwest Research Institute https://orcid.org/0000-0002-2686-4937

Research Article

Keywords: Satellite communication, physical layer security (PLS), information hiding, chaotic frequency-hopping, MFSK, jamming

Posted Date: June 23rd, 2022

DOI: https://doi.org/10.21203/rs.3.rs-1748674/v1

Enhancing Physical Layer Security via Information Hiding and Chaotic Frequency-Hopping Signal

MingQuan Fan[1]

Southwest China Research Institute of Electronic Equipment, Chengdu, China

Abstract: With the development of super computation ability and invention of quantum computer, the conventional calculation quantity based encryption system suffers great impact. Safeguarding data confidentiality in physical layer of wireless satellite communication system has attracted many eyes from academia and industry. In this paper, we propose a groundbreaking revolution method to enhance physical layer security (PLS) by information hiding technique, that is, embedding secret information into chaotic frequency-hopping signal using MFSK modulation. First, secret information to be transmitted is encrypted with chaotic binary sequence. Secondly, according to frequency-hopping pattern, select suitable modulation order and specific frequency corresponding to each encrypted data block under chaotic address sequence. Finally, the encrypted information is embedded into frequency-hopping Sine signal by MFSK modulation. The experimental results indicate that the proposed scheme is robust against various jamming attacks, such as power attenuation, noise adding, single-tone jamming, key exhaustive search, etc.

Keywords: Satellite communication, physical layer security (PLS), information hiding, chaotic frequency-hopping, MFSK, jamming

1. Introduction

Satellite communication systems have ability to transmit information over long distances without the restriction of geographical environment, and have been widely used in military and civilian applications[1,2], such as command control, hydrometeorology, remote sensing, video broadcasting, etc, which brings great convince and becomes the indispensable part to people's lives. However, the openness of wireless satellite communication channel makes it be susceptible to interception and eavesdropping at any time[3,4]. Currently, majority of traditional methods utilize cryptographic techniques and related protocols to protect information confidentiality. The traditional cryptographic techniques encrypt import or private information for safeguarding data confidentiality using high computation capacity. Nevertheless, these standardized cryptographic algorithms and related protocols are well-known to all users and attackers, their drawbacks are well researched[5,6], the attackers just lack high computation costs. With the development of super computation ability and the invention of quantum computer, the conventional calculation quantity based encryption system suffers great impact, besides, deploy traditional encryption methods with higher complexity will increase system hardware and software requirements of satellite communication networks, it is unpractical. Therefore, how to protect data confidentiality of satellite communication links with low cost and high efficiency is really an urgent and valuable problem, and there is a paucity of literature on this theme[7,8]. Under such background, physical layer security (PLS) has attracted more attention in recent years, and novel information theory based security approaches focus on physical layer security issues are experiencing explosive growth[9-16].

[1] Corresponding author. (E-mail address: 1147955679@qq.com)

Ref.[9] proposed a new scheme for satellite communication using cooperative relay system. They adopted cooperative communication technique to improve channel quality of the desired main channel, meanwhile reduce the channel quality of the eavesdropping channel, in this way, the security capacity D-value between eavesdropping channel and main channel was expanded. To strengthen the hybrid satellite terrestrial relay networks security against wiretapping attack, Ref.[10] present a strategy of joint opportunistic relay selection and threshold employment based on user scheduling scheme, and it was used to balance system performance and implementation complexity. Ref.[11] utilized relays for cooperative jamming, and with the total power constraint of relays, the jamming signals were optimized to maximize the secrecy rate. First, the maximal ratio transmission scheme was used to maximize the secrecy rate, then based on the framework of power gain region, the optimal jamming scheme could be obtained via efficient one-dimensional searching method by interpolating between two sub-optimal solutions. However, these approaches[10,11] do not suitable to inter-satellite link transmission. Ref.[12] proposed optimal user-relay pair selection standard for minimizing secrecy outage probability (SOP). Furthermore, the asymptotic SOP expressions at high SNR regime and the insights in terms of achievable diversity order were obtained, which elaborated the impact of various channel/system parameters on secrecy performance of a downlink hybrid satellite-terrestrial relay network. Ref.[13] developed an analytical framework for the performance evaluation and prediction of non-geostationary orbit satellite communication systems. The expressions of secrecy capacity and secrecy outage probability were obtained in closed-form. They proved how satellite elements and rain attenuation affect the communication security performance, but they did not give the suitable countermeasures. Ref.[14] developed a methodology for the practical design of a secure satellite physical layer. Make use of existing hash codes and error correcting codes, the proposed method constructed practical wiretap channel codes. However, when the eavesdropper was situated physically close to the antenna transmitter, the secure communication could not be guaranteed. Ref.[15] proposed a threshold-based scheduling scheme with the assumption of colluded and collaborated eavesdropping scenarios. Specifically, in order to get further insights of the proposed scheduling scheme at high level signal-to-noise ratios, they asymptotically analyzed the performance of secrecy outage probability (SOP) and average secrecy capacity (ASC). Ref.[16] given a secure communication model based on collaboration with the interference relay of satellite physical layer. Relay selection and power allocation were further investigated to enhance the security performance. With instantaneous channel state information (CSI) and statistical CSI conditions, the relay selection standard was obtained to minimize the secrecy outage probability (SOP) for suitable power allocation factor.

In this paper, in order to enhance the PLS of wireless satellite communication system links, we propose a groundbreaking revolution method to transmit secret information by information hiding technique and chaotic frequency-hopping signal. Compared with previous schemes, we hide the secret information into the specific frequency point of MFSK modulation, even if the eavesdroppers demodulate corresponding frequency points, they cannot obtain the corresponding secret information for the adoption of information hiding technique and chaos based frequency-hopping pattern. The novel stego-wave design method is suitable to any link of wireless satellite communication system.

The reminder of this paper is organized as follows. Section 2 elaborates the details of secret information embedding and stego-wave generation. Section 3 describes how to extract the

embedded secret information with chaotic frequency-hopping pattern. The experimental results and analysis are given in Section 4. We draw our conclusions in Section 5.

2. Secret Information Embedding and Stego-Wave Generation

In this section, we focus on the novel MFSK modulation method to embed secret information and generate stego-wave. The proposed method is suitable to uplink, downlink, and inter-satellite link of wireless satellite communication system. Suppose $I=\{I(i,j)\}$, $1\le i\le M$, $1\le j\le N$, represents the secret information, here, M and N are as the number of pixels for every column and row, respectively. The secret information embedding and stego-wave generation is illustrated in Fig.1. Details of embedding are elaborated as following:

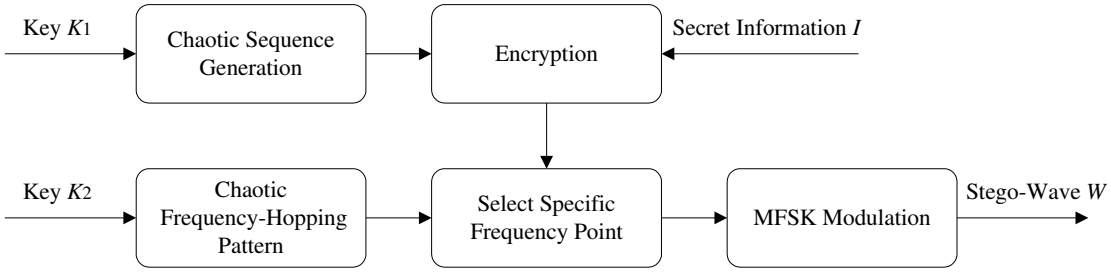

Fig.1. The sketch map of secret information embedding and stego-wave generation.

Step1. Chaotic Sequence Generation. Based on key K_1, use Logistic map to generate pseudo-random sequence $P=\{P(r)\in(0,1)\}$, $r=1,2,\cdots,M\times N$, here, K_1 is the initial value of the adopted chaotic system. According to the quantization rule shown in Eq.(1), the binary chaotic sequence $B=\{B(r)\in\{0,1\}\}$ is obtained.

$$B(r)=\begin{cases}1 & if\ P(r)\ge 0.5\\ 0 & if\ P(r)<0.5\end{cases} \tag{1}$$

Step2. Encryption. First, covert the secret information I to 1-D vector $V=\{V(k)=I(i,j)\}$, $k=(i-1)\times N+j$. Then the 1-D vector V is XORed with binary chaotic sequence B to generate encrypted information stream E, described as Eq.(2) shows.

$$E=V\oplus B \tag{2}$$

where, $E=\{E(r)\in\{0,1\}\}$.

Step3. Chaotic Frequency-Hopping Pattern. First, according to frequency-hopping range $[fb,fe]$, here, fb and fe are the start frequency point and end frequency point, the number of frequency-hopping points $nu=(fe-fb)/deltaf$, here, $deltaf$ is the frequency-hopping interval. The total frequency center points f_{r_0} of each frequency-hopping interval are constructed as a frequency point image $FI=\{FI(i_1,j_1)=f_{r_0}\}$, here, $1\le i_1\le M_1$, $1\le j_1\le N_1$, $r_0=(i_1-1)\times N_1+j_1$, $1\le r_0\le nu$, and it is the frequency interval index, as Fig.2 shows.

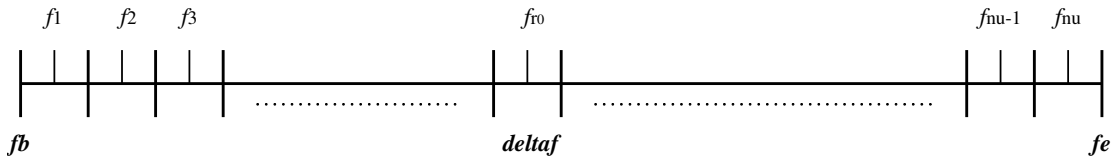

Fig.2. The sketch map of frequency-hopping points distribution.

Then, based on key K_2, use Logistic map to generate pseudo-random sequence $Q=\{Q(r)\,|\,r=1,2,\cdots,M_1\times N_1\}$ with length of $M_1\times N_1$, here, K_2 is the initial value of the adopted chaotic system, M_1 and N_1 are the column and row size of chaotic frequency-hopping pattern, $nu=M_1\times N_1$. In succession, the elements of Q are sorted in descending order, just as Eq.(3) shows.

$$\left\{Q_{a(1)},\cdots,Q_{a(r_0)},\cdots,Q_{a(M_1\times N_1)}\right\}=\text{descend}\left\{Q(1),\cdots,Q(r),\cdots,Q(M_1\times N_1)\right\} \tag{3}$$

where, $a(r_0)$ is the address index of the sorted chaotic sequence, $1\le a(r_0)\le M_1\times N_1$. Finally, according to address index sequence, the chaotic frequency-hopping pattern FH is obtained as follows.

$$FH(p_1,q_1)=FI(m,n) \tag{4}$$

where,

$$p_1=\begin{cases}\lfloor a(r_0)/N_1\rfloor, & if\ \mathrm{mod}(a(r_0),N_1)=0\\ \lfloor a(r_0)/N_1\rfloor+1, & if\ \mathrm{mod}(a(r_0),N_1)\neq 0\end{cases} \tag{5}$$

$$q_1=\begin{cases}N_1, & if\ \mathrm{mod}(a(r_0),N_1)=0\\ a(r_0)-\lfloor a(r_0)/N_1\rfloor\times N_1, & if\ \mathrm{mod}(a(r_0),N_1)\neq 0\end{cases} \tag{6}$$

and $r_0=(m-1)\times N_1+n$, $m=1,2,\cdots,M_1$, $n=1,2,\cdots,N_1$.

Step4. Select Specific Frequency Point. First, the encrypted information stream E is equally split into non-overlapping blocks with size of b for each block, denoted as $E'(l)$, $l=1,2,\cdots,MN/b$. Then convert binary number $E'(l)$ to decimal number $D(l)$, and $FH(p_1,q_1)$ is select as specific frequency point, p_1 and q_1 are obtained by Eq.(5) and Eq.(6) with $D(l)+1$ replace r_0, and $FH(p_1,q_1)=a(D(l)+1)\times deltaf+fb-deltaf/2$.

Step5. MFSK Modulation. Generate the corresponding waveform according to Eq.(7), and connect all MN/b waveforms to construct the final stego-wave W.

$$S(l)=\text{Sine}(2\times\pi\times FH(p_1,q_1)\times n/N) \tag{7}$$

where, $n=0,\mathrm{K}\ N-1$, N is the FFT (fast Fourier transform) number.

3. Secret Information Extraction Procedure

The secret information extraction has no use for any side information, and it is almost the reverse of embedding process. The overall flowchart is shown in Fig.3, and details are described as

follows.

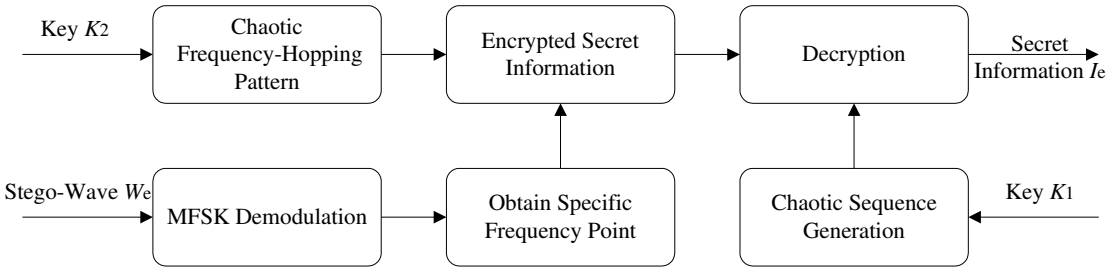

Fig.3. Diagram of secret information extraction procedure.

Step1. Chaotic Frequency-Hopping Pattern. According to Step3 in Section 2, based on key K_2, we get the chaotic frequency-hopping pattern $FH=\{FH(p_1,q_1)\}$, $1\le p_1\le M_1$, $1\le q_1\le N_1$.

Step2. MFSK Demodulation. The pseudo-code of this step is illustrated as follows.

```
Nyquist=N/2-1
f=FFT(wa)
fn=abs(f)×2/N
x=fn(1:Nyquist)
[value,index]=sort(x,'descend')
f0=index(1)-1
```

where, N is the FFT number, wa is a piece of waveform corresponding to one specific frequency point, function $\mathrm{abs}(\mathrm{g})$ represents getting the absolute value, $\mathrm{sort}(\mathrm{g}'descend')$ means sorting sequence with the sorted value and corresponding index as results according to descending order, f_0 is the frequency point corresponding to the piece of waveform wa.

Step3. Encrypted Secret Information. According to chaotic frequency-hopping pattern FH and corresponding specific frequency point f_0 to each piece of waveform, find the position of f_0 in frequency-hopping pattern FH, denote its position as (i_1,j_1), then $a(r_0)=(i_1-1)\times N_1+j_1$. With sorted pseudo-random sequence $Q=\{Q(r)\}$, $r=1,2,\cdots,M_1\times N_1$, r_0 is obtained, and convert decimal number r_0-1 into binary sequence b_0, connect all binary sequences b_0 of each piece of waveform to form the extracted encrypted information E'.

Step4. Chaotic Sequence Generation. According to Step1 in Section 2, based on key K_1, we get the binary chaotic sequence B.

Step5. Decryption. To obtain the original secret information V', perform XOR operation between binary chaotic sequence B and the extracted information E', as Eq.(8) shows.

$$V'=E'\oplus B \tag{8}$$

where, $V'=\{V'(r)\in\{0,1\}\}$, $r=1,\mathrm{K},MN$.

4. Experimental Results and Analysis

In our experiments, a binary image with size of 64×64 is used as the secret information, shown in Fig.4. Other parameters are set as follows: $fb = 25\text{Hz}$, $fe = 12825\text{Hz}$, $deltaf = 50\text{Hz}$, $M = 64$, $N = 64$, the number of frequency intervals is $(fe - fb)/deltaf = 256$, then $b = 8$, $M_1 = 16$, $N_1 = 16$, and the number of FFT is 26000. K_1 ~ K_2 are the initial values of Logistic map, their range is $(0,1)$. In this correspondence, bit error rate (BER) is used to measure the reliability. Its definition is shown as following:

$$\text{BER} = \frac{E_b}{M \times N} \times 100\% \tag{9}$$

where E_b is the number of erroneously detected frequency points. Fig.5 shows the generated stego-wave, and Fig.6 shows the extracted secret information from stego-wave with BER=0.

Fig.4. A binary image used as secret information.

Fig.6. The extracted secret information.

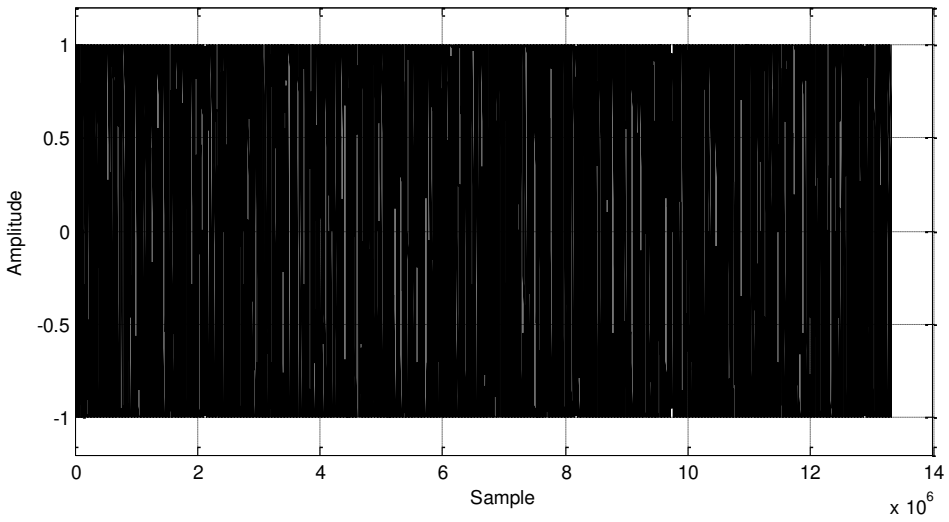

Fig.5. The generated stego-wave.

4.1 Robustness Against Power Attenuation

To wireless satellite communication system, it is common for signals to suffer attenuation under various complex environment, such as propagation distance, rain, obstacle, etc. The proposed scheme hides secret information by frequency modulation, it is connaturally robust against amplitude power attenuation. Table.1 lists the results of extracted binary secret images and its

BERs under various degrees of power attenuation, where “Ratio” means the power ratio between attenuated signal and the original one. Fig.7 shows the attenuated signal with 50% power ration to the original signal. From Table.1, it is easily known that the proposed scheme is most robust against power attenuation.

Table.1. Robustness against power attenuation.

Ratio	100%	90%	80%	70%	60%
BER	0	0	0	0	0
Result					
Ratio	50%	40%	30%	20%	10%
BER	0	0	0	0	0
Result					

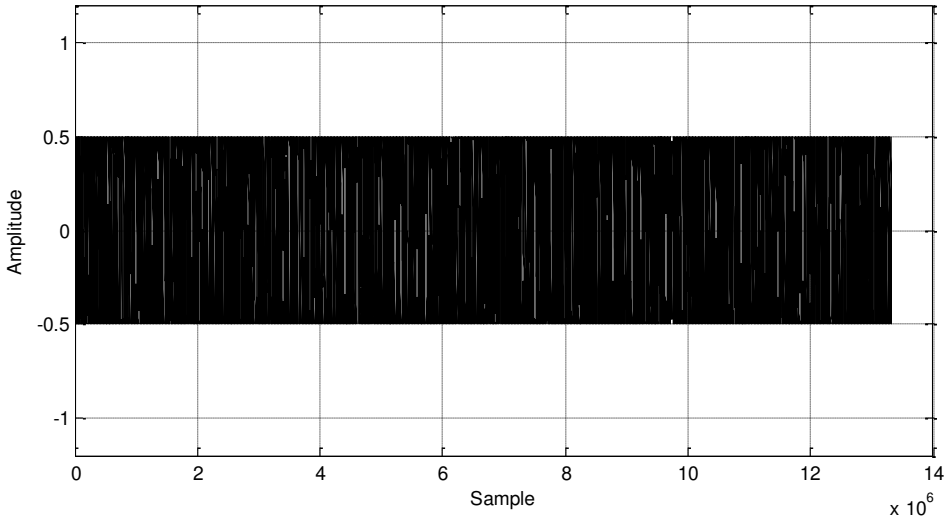

Fig.7. The attenuated signal with 50% degree.

4.2 Robustness Against Noise Adding

Besides the power attenuation, it is also common for signals to suffer noise adding attack. We perform noise adding attack on the generated stego-wave. Specifically, we add white Gaussian noise with different degrees to pollute the generated stego-wave. Table.2 lists the results of extracted binary secret images and its BERs under various SNRs. Fig.8 shows the polluted signal with SNR equals to 5dB. Fig.9 shows the polluted signal with SNR equals to 1dB. From the results, it can be found that we have the ability to extract the secret information correctly with the SNR as low as 1dB. It illustrates that our proposed scheme is extremely robust against noise

adding attack.

Table.2. Robustness against noise adding attack.

SNR(dB)	10	9	8	7	6
BER	0	0	0	0	0
Result					
SNR(dB)	5	4	3	2	1
BER	0	0	0	0	0
Result					

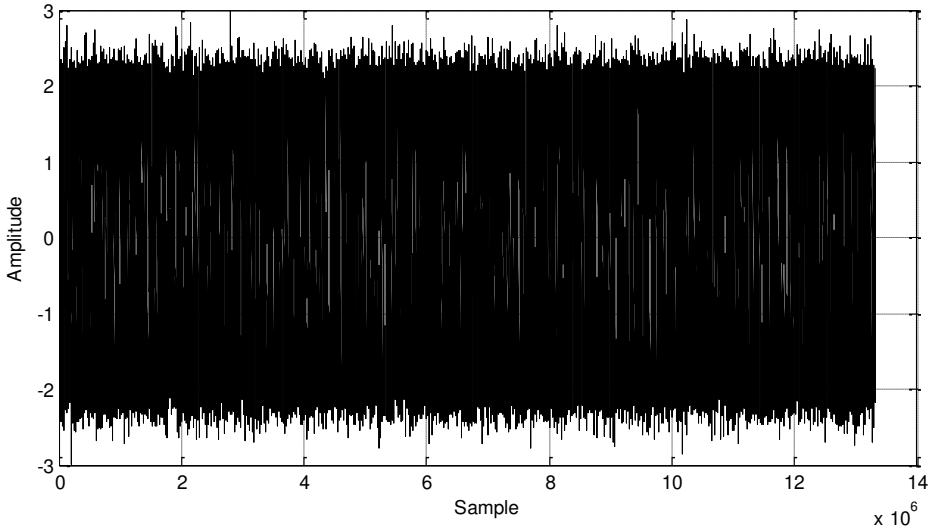

Fig.8. The polluted signal with SNR equals to 5dB.

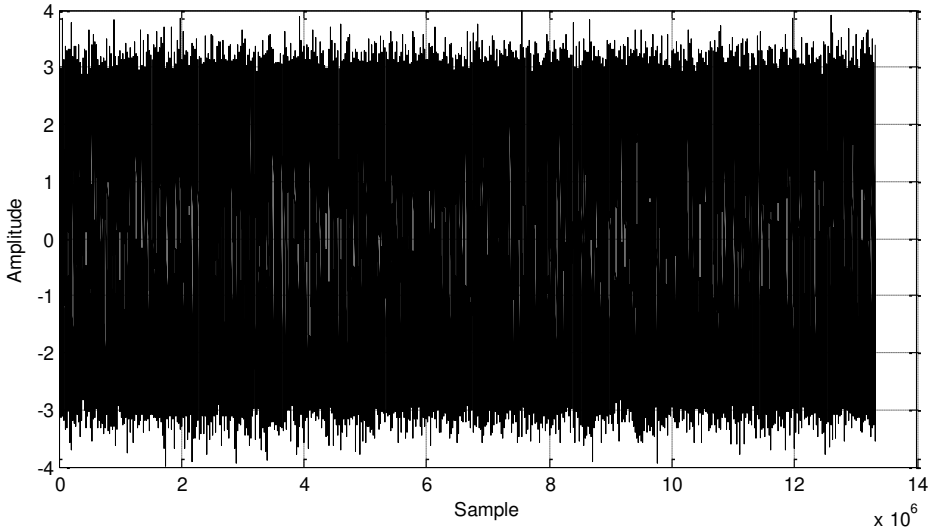

Fig.9. The polluted signal with SNR equals to 1dB.

4.3 Robustness Against Single-Tone Jamming

In this Section, we give the experimental results against single-tone jamming. In real communication environment, the communication links are easily suffering from human interferences, where single-tone jamming is the frequently used method. It means the attacker utilize waveforms with fixed frequency to interfere our generated stego-wave for erroneous extraction of binary secret information. Fig.10 shows the attacked stego-wave with single-tone jamming frequency equals to 975Hz, Fig.11 shows the attacked stego-wave with single-tone jamming frequency equals to 6425Hz. Fig.12 and Fig.13 shows the extracted binary secret information corresponding to Fig.10 and Fig.11, respectively. From the results, we can find the single-tone jamming does not work to our proposed scheme.

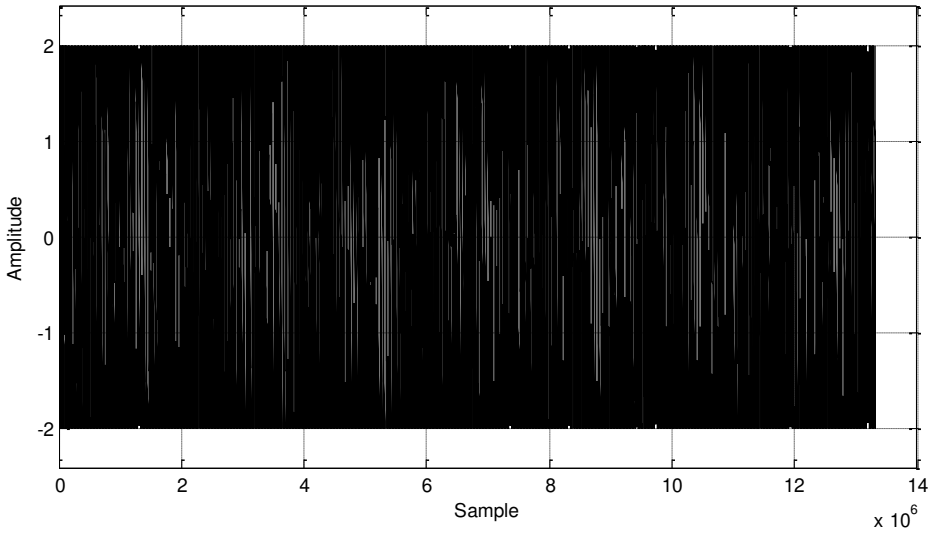

Fig.10. The polluted stego-wave with single-tone jamming frequency equals to 975Hz.

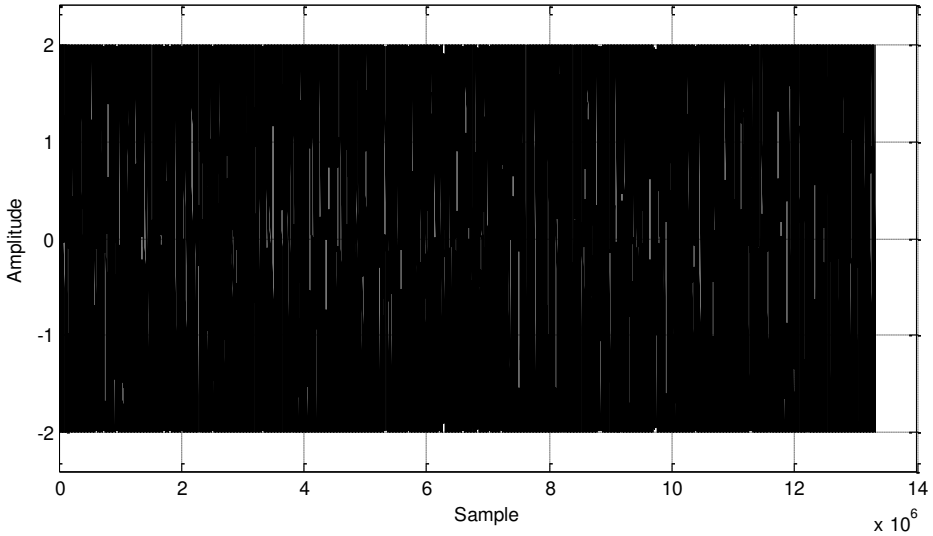

Fig.11. The polluted stego-wave with single-tone jamming frequency equals to 6425Hz.

Fig.12. Extracted secret information(975Hz). **Fig.13.** Extracted secret information(6425Hz).

4.4 Security Analysis

In our proposed scheme, the attacker only guesses most frequency points correctly, then secret information can be extracted from the stego-wave. Suppose that for a segment of stego-wave, the operation of correctly extracting bits is assumed as an independent random variable with probability of p_1. Let N be the total segments, and r be the number of matching segments. Then based on Bernoulli trials assumption, we get

$$p_r = C_N^r \left(p_1\right)^r \left(1-p_1\right)^{N-r} \tag{10}$$

The attacker inteferes the stego-wave successfully if the number of matching segments is greater than a threshold Th. Then the probability of the cases that $r \geq Th$ is the probability of successful jamming, denoted as P. It is defined as:

$$P = \sum_{r=Th}^{N} p_r \tag{11}$$

From Eqs.(10) and (11), we get

$$P = \sum_{r=Th}^{N} C_N^r \left(p_1\right)^r \left(1-p_1\right)^{N-r} \tag{12}$$

According to aforementioned experimental parameters, $N = 64 \times 64 = 4096$, suppose $Th = 0.6N$, here, we suppose that extracting as long as 60% secret information bits correctly, the binary secret image can be distinguished. $p_1 = 1/\left(16 \times 16\right) = 1/256$, Fig.14 gives the probability results when N belongs to (0, 20], and it tells us that the successfully extraction probability P trends to 0 when N is bigger than 4. In our proposed scheme, $N = 4096$, so the successful extraction probability P is approximately equal to 0, which means it is hard for the attacker to guess most frequency points correctly.

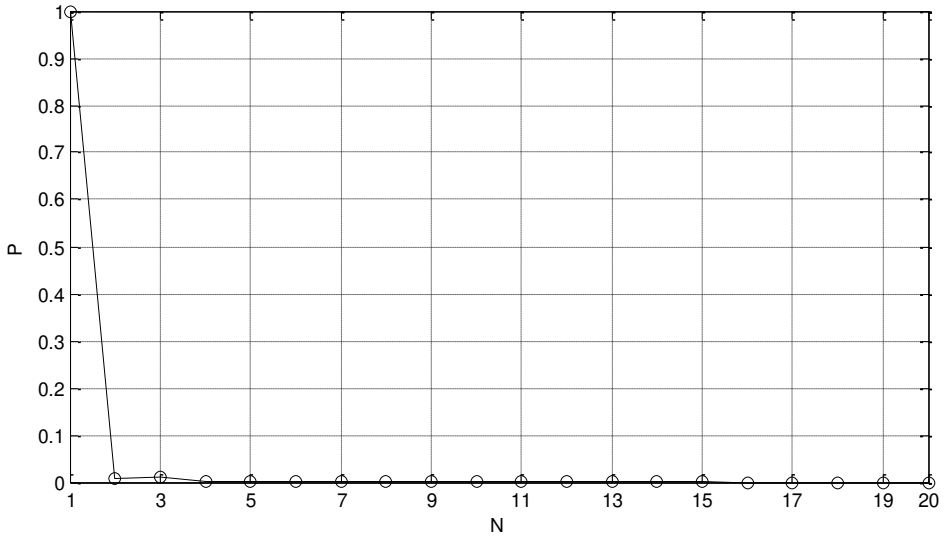

Fig.14. Successful extraction probability P under various N.

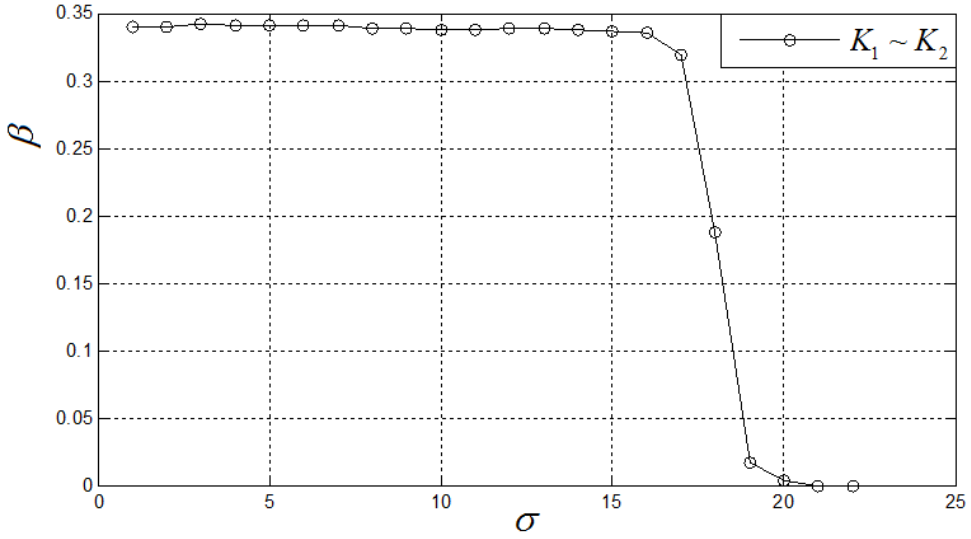

Fig.15. Key space of keys $K_1 \sim K_2$.

If it fails, the attacker can have another way to obtain the whole frequency points, that is, exhaustive searching for system keys. In our scheme, we use chaotic sequences to encrypt secure information (K_1), generate chaotic frequency-hopping pattern (K_2). The keys $K_1 \sim K_2$ are the initial conditions of Logistic map. Because these keys possess real-valued numbers, so a large number of non-periodic noise-like chaotic sequences can be generated. Let $10^{-\sigma}$ represent a micro-change of chaotic key value, then the key space is $1/10^{-\sigma} = 10^{\sigma}$. Here, $\sigma \in Z^+$ is a negative logarithm of changing the chaotic key. As an example, the chaotic sequence x_n is generated by K_1, and another chaotic sequence x'_n is generated by $\left(K_1 + 10^{-\sigma}\right)$. The function $\beta = \sum_{n=0}^{N-1} \left| x_n - x'_n \right| / N$ represents an average distance of two chaotic sequences with a tiny change of K_1, which is used to test the key space. The curve of β is shown in Fig.15. We can

easily see that when the tiny change of $K_1 \sim K_2$ is equal to 10^{-19}, β value is gradually approach zero, which means there are part of chaotic initial parameters can result in the same chaotic sequences. So we know that the key spaces of $K_1 \sim K_2$ are all 10^{19}, and the whole key space of the watermarking scheme is 10^{38}, it is large enough to ensure the security.

5. Conclusions

In this correspondence, we propose a novel scheme for enhancing PLS of wireless satellite communication system by technique of information hiding and chaotic hopping-frequency signal. So far as we known, it is the first time to enhance physical layer communication security by adopting information hiding technique. The experimental results have illustrated the robustness and safe nature of our proposed scheme. The easy operational proposed scheme is practicable for real application environment.

Despite the success of the proposed scheme, it also has a drawback, that is, the proposed scheme obtains embedding frequency points by FFT, which is a bit slow. Therefore, future research will focus on overcoming this problem.

Declarations

The author declares that there are no conflict of interests, I do not have any possible conflicts of interest.

The author declares that no funds, grants, or other support were received during the preparation of this manuscript.

References

[1] D.H. Na, K.H. Park, Y.C. Ko, *et al*. Performance analysis of satellite communication systems with randomly located ground users, IEEE Transactions on Wireless Communications, 2022, vol.21, no.1, pp:621-634.

[2] R. Radhika, W.E. William, A. Fatemeh, *et al*. Survey of inter-satellite communication for small satellite systems: physical layer to network layer view, IEEE Communications Surveys & Tutorials, 2016, vol.18, no.4, pp:2442-2473.

[3] K.F. Guo, K. An, B.N. Zhang, *et al*. Physical layer security for multiuser satellite communication systems with threshold-based scheduling scheme, IEEE Transactions on Vehicular Technology, 2020, vol.69, no.5, pp:5129-5141.

[4] Z. Lin, M. Lin, J. Ouyang, *et al*. Robust secure beamforming for multibeam satellite communication systems, IEEE Transactions on Vehicular Technology, 2019, vol.68, no.6, pp:6202-6206.

[5] D.S. Kundi, A. Khalid, A. Aziz, *et al*. Resource-shared crypto-coprocessor of AES Enc/Dec with SHA-3, IEEE Transactions on Circuits and Systems Ⅰ: Regular Papers, 2020, vol.67, no.12, pp:4869-4882.

[6] Y.C. Niu, J.W. Zhang, A. Wang, *et al*. An efficient collision power attack on AES encryption in edge computing, IEEE Access, 2019, vol.7, pp:18734-18748.

[7] P.Y. Yue, J.P. An, J.K. Zhang, *et al*. On the security of LEO satellite communication systems: vulnerabilities, countermeasures, and future trends, https://arxiv.org/abs/2201.03063.
[8] Y.P. Wu, A. Khisti, C.S. Xiao, *et al*. A survey of physics layer security techniques for 5G wireless networks and challenges ahead, IEEE Journal on Selected Areas in Communication, 2018, vol.36, no.4, pp:679-695.
[9] J. Liu, J.J. Wang, W.X. Liu, *et al*. A novel cooperative physical layer security scheme for satellite downlinks, Chinese Journal of Electronics, 2018, vol.27, no.4, pp:860-865.
[10] K.F. Guo, K. An, B.G. Zhang, *et al*. Physical layer security for hybrid satellite terrestrial relay networks with joint relay selection and user scheduling, IEEE Access, 2018, vol.6, pp:55815-55827.
[11] S. Yan, X.Y. Wang, Z.L. Li, *et al*. Cooperative jamming for physical layer security in hybrid satellite terrestrial relay networks, China Communications, 2019, pp:154-164.
[12] V. Bankey, P.K. Upadhyay. Physical layer security of multiuser multirelay hybrid satellite-terrestrial relay networks, IEEE Transactions on Vehicular Technology, 2019, vol.68, no.3, pp:2488-2501.
[13] Y.Q. Xiao, J. Liu, Y.L. Shen, *et al*. Secure communication in non-geostationary orbit satellite systems: a physical layer security perspective, IEEE Access, 2019, vol.7, pp:3371-3382.
[14] A.V. Castro, M. Hayashi. Physical layer security for RF satellite channels in the finite-length regime, IEEE Transactions on Information Forensics and Security, 2019, vol.14, no.4, pp:981-993.
[15] K.F. Guo, K. An, B.N. Zhang, *et al*. Physical layer security for multiuser satellite communication systems with threshold-based scheduling scheme, IEEE Transactions on Vehicular Technology, 2020, vol.69, no.5, pp:5129-5141.
[16] J.T. Li, S. Han, X.X. Tai, *et al*. Physical layer security enhancement for satellite communication among similar channels: relay selection and power allocation, IEEE Systems Journal, 2020, vol.14, no.1, pp:433-444.