Type of the Paper (Article, Review, Communication, etc.)

Hiding Stealth Optical CDMA Signals in Public BPSK Channels for Optical Wireless Communication

Chih-Ta Yen [1,*], Jen-Fa Huang [2] and Wen-Zong Zhang [3]

[1] Department of Electrical Engineering, National Formosa University, Yunlin, Taiwan, ROC; chihtayen@gmail.com
[2] Department of Electrical Engineering, National Cheng Kung University, Tainan, Taiwan, ROC; huajf@ee.ncku.edu.tw
[3] Department of Photonics Engineering, National Cheng Kung University, Tainan, Taiwan, ROC; qpz189@hotmail.com
* Correspondence: chihtayen@gmail.com; Tel.: +886-5-6315625

Abstract: A new optical steganography scheme is proposed that transmits a stealth optical code-division multiple-access (OCDMA) signal through a public binary phase-shift keying (BPSK) channel. Polarization beam splitters and arrayed waveguide gratings are used to implement a spectral-polarization coding (SPC) system with an incoherent optical source. We employ a Walsh–Hadamard code as the signature code of the user who wants to transmit stealth information using the system. A free space optical link applied to this system maintains the polarization states of light during propagation. The secret data is extracted using correlation detection and balanced subtraction in the OCDMA decoder of the intended receiver, and the other signal from the public channel is reduced by the OCDMA decoder. At the demodulator of the public channel, BPSK demodulation eliminates the stealth signal so that the public channel is not affected by the stealth signal. The two signals cannot interfere with each other. The results of this study show that our proposed optical steganography system is highly secure. The stealth signal can be favorably hidden in the public channel when the average source power of the stealth signal, public noise, and public signal are −5, −3, and 0 dBm, respectively.

Keywords: optical steganography; optical code-division multiple-access (OCDMA); free space optics (FSO); chirped fiber Bragg grating (CFBG).

1. Introduction

With the increasing application of computers in different areas of life and work, information security has become an important concern. To enhance security in the physical layer of an optical network, several approaches have been investigated, such as quantum private communication, optical encryption, and optical steganography [1-4]. Steganography is one of the methods that have received attention in recent years. The word steganography, which is derived from Greek, literally means “covered writing.” The main goal of steganography is to hide information sufficiently well such that any unintended recipients do not suspect that the steganographic medium contains hidden data [5]. This is a major distinction between steganography and the other methods of improving security. For example, optical encryption allows a signal to be encrypted with low latency; thus, the recipient requires a key to read the information. However, each person notices the information by seeing the coded signal; that is, the method cannot prevent the signal from being detected. In some cases, the system is already in danger of being decrypted if an eavesdropper knows about the existence of the signal. Steganography provides an additional layer of security by hiding the data transmission underneath the steganographic medium.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 21 August 2018 doi:10.20944/preprints201808.0367.v1

Peer-reviewed version available at Appl. Sci. 2018, 8, 1731; doi:10.3390/app8101731

Steganography operations have been performed on different cover media such as images, audio, text, and video [6]. In recent years, new research into methods for secure communication over existing public fiber-optic networks has been conducted. Using a concept similar to steganography, the secure signal is processed by a particular technique called optical steganography and can be hidden under the noise floor of a public network. Optical steganography is realized by transmitting a private signal hidden in the existing public channel to increase the secrecy of the communication system. One of the first methods using the concept of optical steganography was proposed by Wu and Narimanov [7-8]. In this method, the signal is hidden using spread spectrum techniques. Several researchers have worked with various secret transmissions over different types of public network. For example, Kravtsov (2007) proposed a method of secure stealth transmission over a wavelength-division multiplexing (WDM) network [9]. Wu (2008) discussed coherent spectral-phase-encoded OCDMA signal transmission in a WDM network [10]. Wang (2011) investigated stealth transmission over a public differential phase-shift keying (DPSK) channel [11]. Tait and Wu (2014) demonstrated an optical steganography technique based on amplified spontaneous emission noise [12].

The basic approach of optical steganography is to temporally stretch the pulses of a signal using high-dispersion elements. The amplitudes of the signal pulses are dramatically decreased after the stretching so that the signal can be hidden underneath the public signal and system noise. However, once the existence of the hidden channel is revealed, eavesdroppers may take measures to process the stealth signal; therefore, the stealth channel may be weak against eavesdropping. To enhance the security of the stealth channel, additional security measures are required against eavesdroppers. For this, optical code-division multiple-access (OCDMA)—which has been successfully applied in optical steganography—is a great choice [13-15].

In this study, the stealth signal was encoded using a spectral-polarization-coded OCDMA (SPC-OCDMA) technique, which employs polarization beam splitters (PBSs) and arrayed waveguide gratings (AWGs) as the encoders and decoders. Chirped fiber Bragg gratings (CFBG) were used as the pulse stretcher and compressor to implement optical steganography. To restore the stealth signal, the public signal was removed using the balanced correlation detection/subtraction mechanism conventionally adopted in OCDMA decoders. A binary phase-shift keying (BPSK) demodulator was used to reject stealth OCDMA interference and system noise. Thus, the stealth signal and noise affect the public network only slightly.

2. Theories and Principles

2.1. Chromatic dispersion

Chromatic dispersion in an optical medium is a phenomenon in which the group velocity of light propagating through the medium depends on the light's wavelength. Let us consider a situation wherein a pulse is transmitted along a single-mode fiber. In an optical fiber, different spectral components of the pulse travel with slightly different group velocities. Consequently, they arrive at the fiber output at different times, even though they started at the same time. Figure 1 illustrates the phenomenon of chromatic dispersion caused by light propagation in a single-mode fiber. A pulse at frequency ω passes through a fiber with length L after a time delay $\tau = L/v_g$. The group velocity v_g is given by

$$v_g = d\omega/d\beta\,, \tag{1}$$

where β is the propagation constant. The range of pulse broadening for a fiber of length L can be expressed as [16]

$$\Delta\tau = \frac{d\tau}{d\omega}\Delta\omega = \frac{d}{d\omega}\left(\frac{L}{v_g}\right)\Delta\omega = L\frac{d^2\beta}{d\omega^2}\Delta\omega\,, \tag{2}$$

where $\Delta\omega$ is the spectral width of the pulse. $\Delta\omega$ is usually replaced by the range of wavelengths $\Delta\lambda$ emitted by the optical source. Then, Eq. (2) can be written as

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 21 August 2018 doi:10.20944/preprints201808.0367.v1

Peer-reviewed version available at Appl. Sci. 2018, 8, 1731; doi:10.3390/app8101731

$$\Delta\tau = -(2\pi c/\lambda^2)\beta'' L\Delta\lambda = DL\Delta\lambda, \tag{3}$$

by using the relations $\omega = 2\pi\ c/\lambda$ *and* $\Delta\omega = (-2\pi c/\lambda^2)\Delta\lambda.$, where β'' is the second derivative with respect to λ and D is the *dispersion parameter* with units ps/(nm.km). A negative dispersion parameter indicates that light with a longer wavelength travels faster than that with a shorter wavelength.

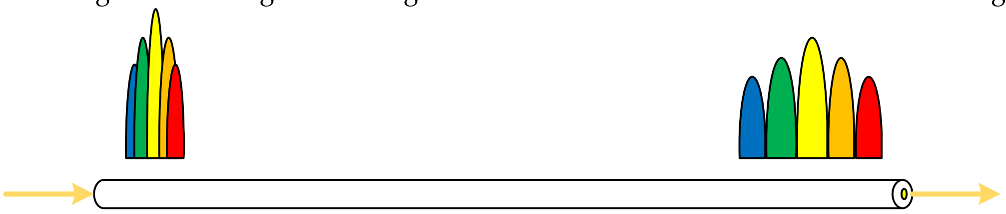


Figure 1. Broadening of light along a single-mode fiber.

2.2. Spectral-polarization coding using Walsh–Hadamard codes

In spectral amplitude coding (SAC)-OCDMA systems, a specific signature address code is assigned to each user to code the amplitude of the source spectrum. Walsh–Hadamard codes are quasi-orthogonal codes used in SAC-OCDMA systems [17-18] and are obtained by selecting the row of the Walsh–Hadamard matrix comprising elements {1,0}. Each row except the first row contains $N/2$ zeros and $N/2$ ones, where N is the length of the codeword. An $N \times N$ Walsh–Hadamard matrix can be generated using the recurrence relation, which is given by

$$H_N = \begin{bmatrix} H_{N/2} & H_{N/2} \\ H_{N/2} & \overline{H}_{N/2} \end{bmatrix}, \tag{4}$$

It is clear that the autocorrelation value is $N/2$ and the cross-correlation value between different rows is $N/4$. Let us introduce the Walsh–Hadamard code correlation properties as follows:

$$R_{cc}(k,l) = \sum_{i=1}^{N} c_k(i)c_l(i) = \begin{cases} N/2, k = l \\ N/4, k \neq l \end{cases}, \tag{5}$$

and

$$R_{c\bar{c}}(k,l) = \sum_{i=1}^{N} c_k(i)\bar{c}_l(i) = \begin{cases} 0 \quad\ , k = l \\ N/4, k \neq l \end{cases}, \tag{6}$$

where C_k is the code sequence in the kth row of the Walsh–Hadamard matrix. According to the property $R_{CC}(k,l) = R_{C\bar{C}}(k,l)$ for $k \neq l$, a receiver is designed to perform correlation subtraction expressed as $R_{CC}(k,l) - R_{C\bar{C}}(k,l)$:

$$Z = R_{CC}(k,l) - R_{C\bar{C}}(k,l) = \begin{cases} N/2\ ,\ \mathrm{k} = \mathrm{l} \\ \quad 0\quad ,\ \mathrm{k} \neq \mathrm{l} \end{cases}, \tag{7}$$

This equation shows that the influence from other users will be rejected.

In the SPC scheme, the source spectrum is encoded by orthogonal polarizations according to the specific signature address code. We employed a Walsh–Hadamard code to allocate a vertically or horizontally linear state of polarization (SOP) to each specified wavelength. The specific code sequence for the SPC-OCDMA system comprises Ck(H) and $\overline{\mathrm{C}_\mathrm{k}}$(V), where H and V denote the vertical and horizontal polarization, respectively.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 21 August 2018 doi:10.20944/preprints201808.0367.v1

Peer-reviewed version available at Appl. Sci. 2018, 8, 1731; doi:10.3390/app8101731

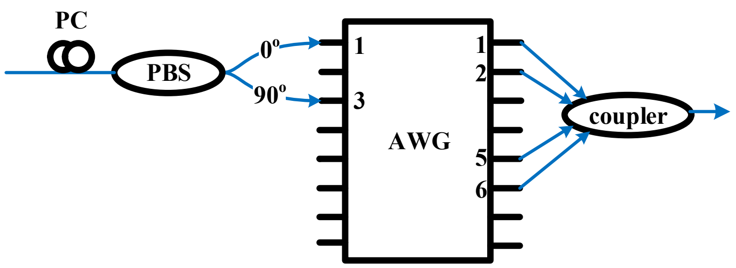


Figure 2. Structure of SPC-OCDMA encoder.

As shown in Figure 2, using the wavelength cyclic-shifted characteristic property of AWG routers represented in Eq. (8), we can obtain C (H) = (1, 1, 0, 0, 1, 1, 0, 0) and $\overline{C}(V)$ = (0, 0, 1, 1, 0, 0, 1, 1) to form the SPC code. C (H) and $\overline{C}(V)$ correspond to code patterns (λ_{1H}, λ_{2H}, 0, 0, λ_{5H}, λ_{6H}, 0, 0) and (0, 0, λ_{3V}, λ_{4V}, 0, 0, λ_{7V}, λ_{8V}), respectively. Therefore, the wavelength-coding patterns of the SPC code are (λ_{1H}, λ_{2H}, λ_{3V}, λ_{4V}, λ_{5H}, λ_{6H}, λ_{7V}, λ_{8V}) when a data bit 1 is transmitted and (0, 0, 0, 0, 0, 0, 0, 0) when a data bit 0 is transmitted. The subscripts of λij denote the ith wavelength encoded and the SOP:

$$(\#\text{input port} + \#\text{output port} - 1) \bmod N = \#\text{wavelength}, \tag{8}$$

2.3. Chirped fiber Bragg gratings

As described in Section II-A, dispersion leads to the pulse broadening of optical pulses propagating along a fiber and becomes a limiting factor for optical communication systems operating at high bit rates. Herein, we use the characteristics of dispersion to stretch the pulse; this transforms the stealth signal into a noise-like signal so that it can be buried in a public channel.

Figure 3 shows the structure of a CFBG [19]. A fiber Bragg grating is a periodic perturbation of the refractive index along the fiber length. The core of the fiber is exposed to an intense optical interference pattern to fabricate the Bragg gratings. When the incident light passes through the periodic structure, a narrow band of the optical field is reflected by continuous, coherent scattering from the variations in the refractive index. The strongest interaction occurs at the Bragg wavelength λ_B, which is given by

$$\lambda_B = 2 n_{eff} \Lambda , \tag{9}$$

where n_{eff} is the effective refractive index of the core and Λ is the grating period. The chirping of a fiber Bragg grating indicates changes in the period of the grating with distance.

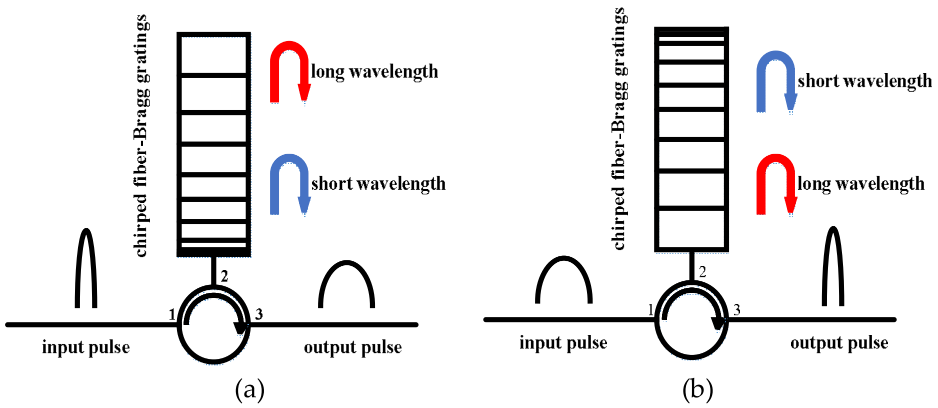


Figure 3. Structure of CFBG providing (a) positive dispersion and (b) negative dispersion.

As depicted in Figure 3(a), the grating period increases along the fiber's length so that shorter wavelengths are reflected nearer the input of the fiber whereas longer wavelengths are reflected nearer the output. Thus, light with longer wavelengths is more delayed than light with shorter

Peer-reviewed version available at Appl. Sci. 2018, 8, 1731; doi:10.3390/app8101731

wavelengths. This CFBG structure produces positive dispersion. In contrast to positive dispersion, the structure of the CFBG in Figure 3(b) produces negative dispersion. CFBGs can provide a large dispersion with a small size. To provide the same dispersion in a standard single-mode fiber, the required length must be increased by a factor of 2000 [20], which can make the system more compact.

2.4. Free space optical communication (FSO)

FSO is an optical communication technique for transmitting data in free space, such as air, vacuum, or outer space. The setup of an FSO system is similar to that of an optical fiber cable (OFC) network. The only difference between them is that the optical beams in an FSO network are transmitted through free air compared with glass in OFC networks. As shown in Figure 4, the fundamental structure of an FSO system comprises a laser, an electro-optic modulator (EOM), a lens design, and a detector. The laser is modulated using the EOM and the laser beam is converged onto the receiver by the lens.

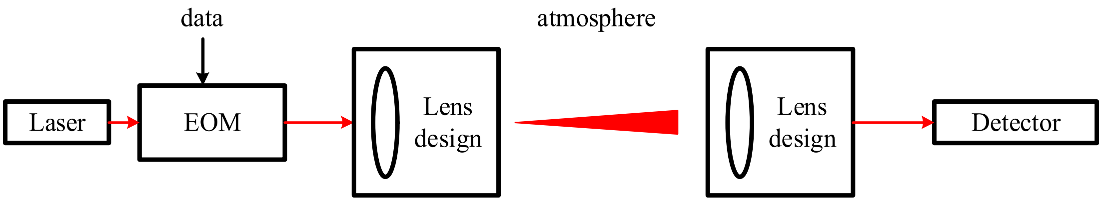


Figure 4. Structure of FSO system.

FSO system performance is dependent on the transmission medium because of the presence of foreign elements such as rain, fog, haze, physical obstructions, scattering, and atmospheric turbulence [21].

3. Experiment Setup and Results

The SPC-OCDMA system was simulated using Opti-System software (v 7.0). Opti-System is a software simulation kit from Optiwave™ that analyzes the performance of optical systems and networks. A schematic of the experimental setup is presented in Figure 5. The stealth signal is first encoded and then transmitted into the public channel. To simulate the system noise in a real optical network, a noise source is introduced to generate noise and couple it to the public and stealth signals. This enables convenient investigation of the impact of system noise on the stealth signal.

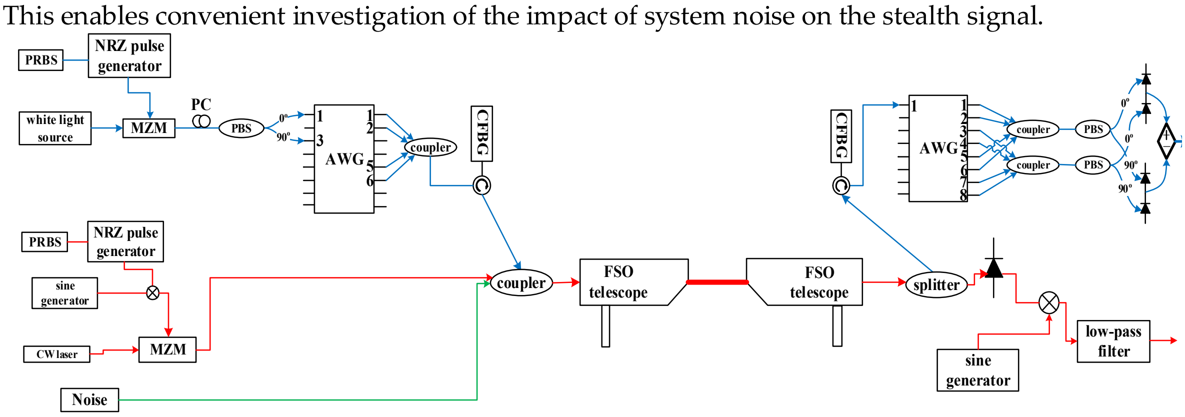


Figure 5. Schematic of optical steganography transmission system.

3.1. Structure of public and stealth channels

BPSK is the simplest form of the phase-shift keying technique and is a digital modulation method that transmits data by changing the phase of the carrier wave. The phase difference of the carrier wave is 180° when transmitting data bits 1 and 0. Furthermore, the frequency of the carrier wave is typically 10 times the bit rate. We transmit a BPSK signal in the public channel to make the signal always exist irrespective of the data bit transmitted. The stealth signal is not exposed because of the disappearance of the public signal. Figure 6 presents the structure of the public channel.

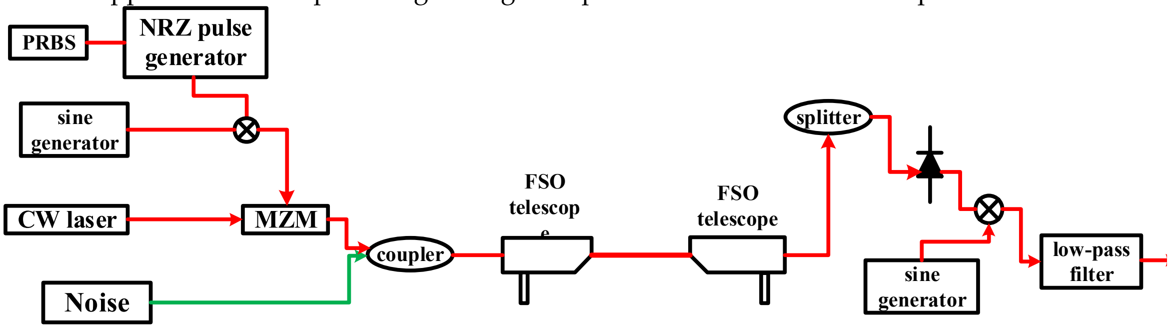


Figure 6. Schematic of BPSK public channel.

In this structure, NRZ pulses are multiplied by a sinusoidal wave and the BPSK signal is generated. The following equation shows the general form of the BPSK signal:

$$S_b(t) = \sqrt{\frac{2E_b}{T_b}} \cos[2\pi f_c t + \pi(1-b)],\ b = 0,\ 1. \tag{10}$$

From the general form, we can conclude that binary data is conveyed using the following signals:

$$S_1(t) = \sqrt{\frac{2E_b}{T_b}} \cos(2\pi f_c t),\ \text{for bit 1,} \tag{11}$$

$$S_0(t) = \sqrt{\frac{2E_b}{T_b}} \cos(2\pi f_c t + \pi) = -\sqrt{\frac{2E_b}{T_b}} \cos(2\pi f_c t + \pi),\ \text{for bit 0,} \tag{12}$$

where E_b is the energy per bit, T_b is the 1-bit duration, f_c is the frequency of the carrier wave, and b is the data bit. Then, the BPSK signal drives a Mach–Zehnder modulator (MZM) to modulate a continuous-wave (CW) laser. To demodulate the public BPSK signal, the optical signal is first transformed into an electrical signal by the photodiode, following which the photocurrent is multiplied by $\cos(2\pi f_c t)$:

$$S_1(t)\cos(2\pi f_c t) = \sqrt{\frac{2E_b}{T_b}} \cos(2\pi f_c t)\cos(2\pi f_c t), \tag{13}$$

$$S_0(t)\cos(2\pi f_c t) = -\sqrt{\frac{2E_b}{T_b}} \cos(2\pi f_c t)\cos(2\pi f_c t), \tag{14}$$

The term $\cos(4\pi f_c t)$ is filtered using a low-pass filter. The data bit is recovered by an appropriate thresholder. The transmitter in the stealth channel is illustrated in Figure 7. On–off keying (OOK) data is generated using a white light source, and the MZM is driven by a pseudorandom binary sequence (PRBS). A polarization controller is placed between the modulator and the PBS to adjust the SOP. The modulated signal is divided into mutually orthogonal SOPs by the PBS and then input into the AWG-based OCDMA encoder.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 21 August 2018 doi:10.20944/preprints201808.0367.v1

Peer-reviewed version available at Appl. Sci. 2018, 8, 1731; doi:10.3390/app8101731

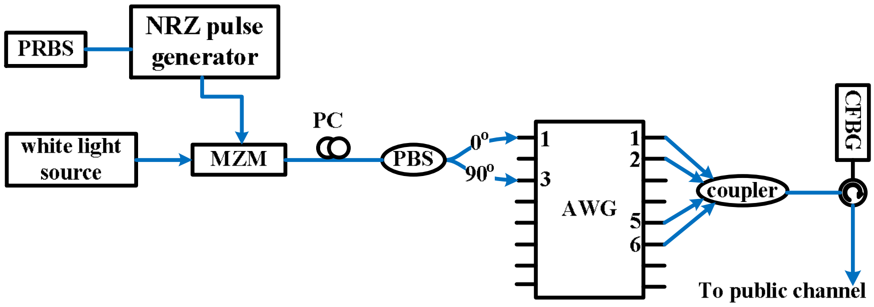


Figure 7. Schematic of stealth channel encoder.

We input two orthogonal SOPs to different AWG input ports. According to the wavelength cyclic-shifted characteristic property of AWG routers detailed in Eq. (8), we can obtain the spectrum encoded by the Walsh–Hadamard code C_k(H) and its complementary code $\overline{C_k}$(V). The encoded stealth signals are combined using a coupler and passed through a CFBG for further pulse broadening to lower the peak power for effectively concealing the stealth channel beneath the public channel.

Figure 8 shows the structure of the proposed SPC decoder. To restore the stealth signal, the received signal is first passed through a CFBG, which is the same as that at the transmitter except with opposite dispersion. The stretched stealth signal is then compressed back into the original profile. Thereafter, the mutually orthogonal SOP components from the encoded spectrum are input to the AWG router for OCDMA decoding. The output ports of the AWG couple with the upper and lower couplers depending on the signature code C_k and its complementary code $\overline{C_k}$. With the PBS, the same SOPs of spectra are extracted for balanced detection. Furthermore, the detected electrical signal from the lower branch is subtracted from the corresponding signal from the upper branch. Finally, the stealth signal is obtained using the decoding mechanism.

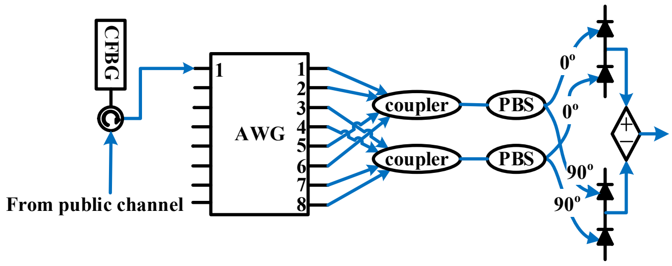


Figure 8. Schematic of stealth channel decoder.

The following equations detail the math analyses of the SPC decoding process. When transmitting data bit 1, the received signal is given by

$$R = C_k(\mathrm{H}) + \overline{C_k}(\mathbf{V}). \tag{15}$$

The spectrum from the upper and lower couplers can be expressed as in Eqs. (16) and (17), respectively:

$$R \cdot C_k = C_k(\mathrm{H}), \tag{16}$$

$$R \cdot \overline{C_k} = \overline{C_k}(\mathrm{V}). \tag{17}$$

According to the proposed structure, the spectra of C_k(H) and $\overline{C_k}$(V) are sent to the topmost and lowest photodiode, respectively. Consequently, the final photocurrent received is described by

$$\sum_{i=1}^{N} C_k(i) - (-\overline{C_k}(i)) = \sum_{i=1}^{N} C_k(i) + \overline{C_k}(i) = N, \tag{18}$$

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 21 August 2018 doi:10.20944/preprints201808.0367.v1

Peer-reviewed version available at Appl. Sci. 2018, 8, 1731; doi:10.3390/app8101731

where N denotes the length of the codeword; here, we assume that each chip of the spectrum produces one unit current.

If another user transmits a signal with Walsh–Hadamard code C_l, the received signal is given by

$$R = C_l(\mathrm{H}) + \overline{C_l}(\mathbf{V}). \tag{19}$$

Then, the spectrum from the upper and lower couplers can be expressed as

$$R \cdot C_k = C_l(\mathrm{H}) \cdot C_k + \overline{C_l}(\mathrm{V}) \cdot C_k, \tag{20}$$

$$R \cdot \overline{C_k} = C_l(\mathrm{H}) \cdot \overline{C_k} + \overline{C_l}(\mathrm{V}) \cdot \overline{C_k}. \tag{21}$$

On the basis of the decoder structure, the spectra of $C_l(\mathrm{H}) \cdot C_k$, $C_l(\mathrm{H}) \cdot \overline{C_k}$, $\overline{C_l}(\mathrm{V}) \cdot C_k$, and $\overline{C_l}(\mathrm{V}) \cdot \overline{C_k}$ are sent to the first to fourth photodiodes, respectively. Consequently, the final photocurrent received can be written as

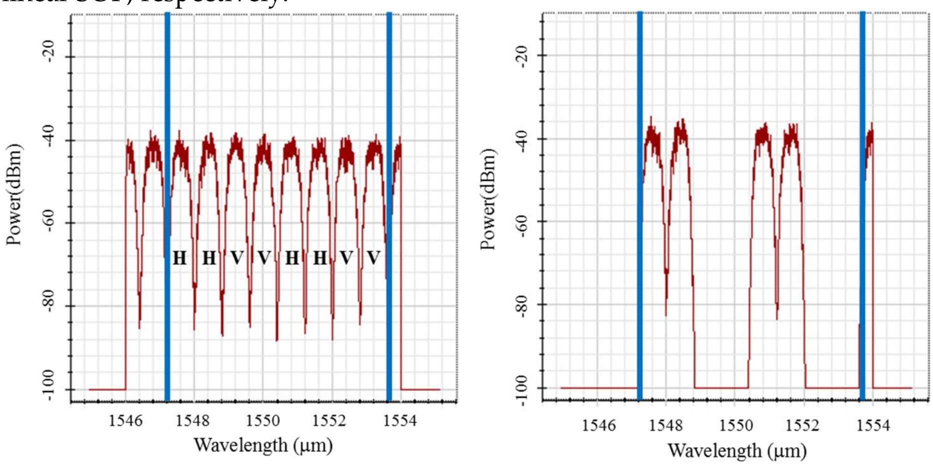
$$\left[\sum_{i=1}^{N} C_l(i)C_k(i) - C_l(i)\overline{C_k}(i)\right] - \left[\sum_{i=1}^{N} \overline{C_l}(i)C_k(i) - \overline{C_l}(i)\overline{C_k}(i)\right] = 0. \tag{22}$$

From the calculations, we observe that the photocurrent is zero at the first balance detection. Thus, only the user with the corresponding code can transmit the signal, with multiuser access interference from other users rejected.

The parameters of the simulation are as follows. To generate the public BPSK signal, an MZM is used to modulate a CW laser at 3 Gbps with a 2^7−1 PRBS. The center wavelength of the CW laser is 1549.2 nm. In the stealth channel, 1-Gbps OOK data is generated using a white light source followed by an MZM driven by a 2^7-1 PRBS. The modulated signal is encoded using an AWG according to a Walsh–Hadamard code with the length of the codeword being 8. We set the codeword to be (1, 1, 0, 0, 1, 1, 0, 0) for the vertical SOP and (0, 0, 1, 1, 0, 0, 1, 1) for the horizontal SOP. The wavelengths utilized are 1547.6, 1548.4, 1549.2, 1550, 1550.8, 1551.6, 1552.4, and 1553.2 nm, respectively.

As discussed in the Introduction, most previous studies on optical steganography have described stealth signals encoded by spread-spectrum OCDMA or phase-encoded OCDMA techniques and transmitted on existing public networks. Therefore, to help fill a gap in knowledge, we investigate the probability of applying other types of OCDMA techniques. The SAC is a promising OCDMA technique that provides high transmission rates with low system complexity and using a low-cost optical source. We compare the proposed SPC with SAC and demonstrate that the proposed SPC-OCDMA system can enhance the security of SAC-OCDMA.

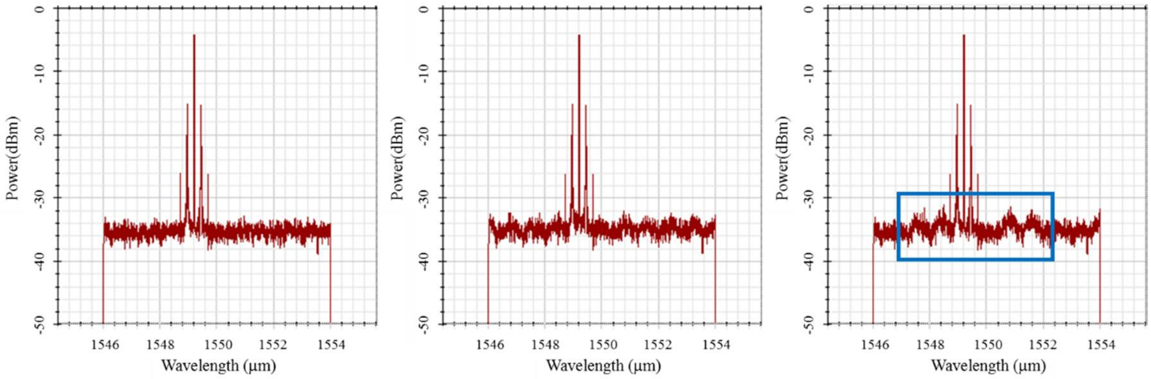
The spectrum of the encoded signal is presented in Figure 9. Figure 9(a) shows the proposed SPC code pattern and Figure 9(b) displays the traditional SAC code. V and H represent vertical and horizontal linear SOP, respectively.



(a) (b)

Figure 9. Spectrum of encoded signal with (a) SPC code and (b) SAC code.

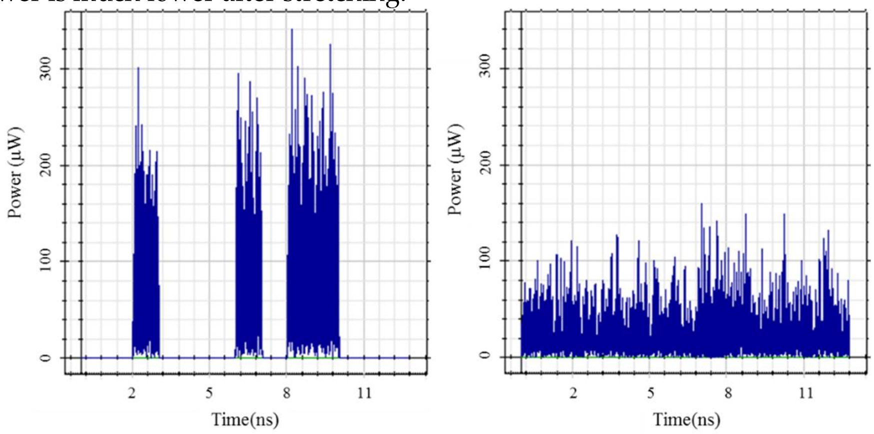
Figure 10 presents the spectrum of the public channel with and without the stealth signal. In Figure 10(a), the peak of the spectrum is the public signal and the other peaks are system noise. Figure 10(b) and (c) indicates that the spectrum of SPC-OCDMA is flatter than that of SAC-OCDMA. In Figure 10(c), the encoded signal is visible near the peak of the public signal. The spectrum of the public channel varies slightly after the SPC signal is transmitted in Figure 10(a) and (b) so that it can be buried in the public channel in the spectral domain.



(a) (b) (c)

Figure 10. Spectrum of public channel (a) without stealth signal; (b) with SPC signal; and (c) with SAC signal.

The encoded stealth signals are combined using a coupler and passed through a CFBG for further pulse broadening to lower the peak power. To effectively conceal the stealth channel beneath the public channel, the CFBG is used to produce a total dispersion of 1600 ps/nm. The waveforms before and after this stretching are displayed in Figure 11, which shows that the pulse is broader and the signal power is much lower after stretching.



(a) (b)

Figure 11. Waveform of stealth signal in time domain (a) before and (b) after pulse broadening.

Figure 12 presents the waveform of the public channel in the time domain. The waveform reveals the necessity of adopting CFBGs. Figure 12(a) and (b) shows that the stealth signal can be favorably hidden in the public channel using a CFBG with 1600 ps/nm dispersion. Without dispersion, the existence of the stealth signal is exposed, as shown in Figure 12(c).

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 21 August 2018 doi:10.20944/preprints201808.0367.v1

Peer-reviewed version available at Appl. Sci. 2018, 8, 1731; doi:10.3390/app8101731

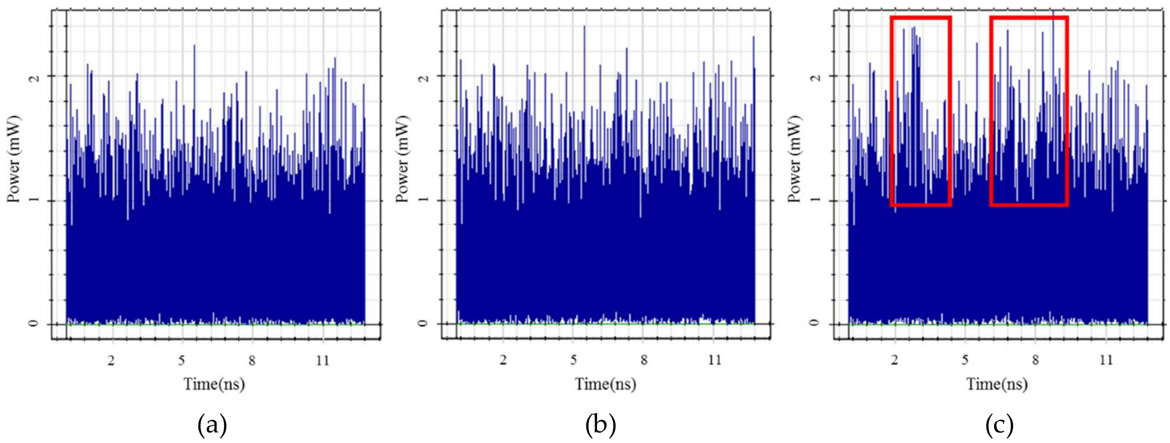


Figure 12. Waveform of public channel in time domain (a) without stealth signal; (b) with stealth signal (1600 ps/nm); and (c) with stealth signal (no dispersion).

The source power of the stealth and public signals are −5 and 0 dBm, respectively. Figures 10 and 12 demonstrate that the spectra and waveform of the public BPSK signal with and without the stealth signal are negligibly different when the noise power is −3 dBm. Therefore, the stealth signal can be buried underneath the system noise and transmitted in the public channel without being detected.

3.2. Interference cancellation of stealth and public signals

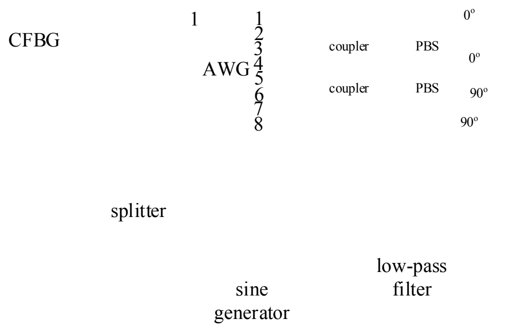


Figure 13. Decoder of SPC stealth signal and demodulator of public signal.

At the receiver side, a 3-dB optical coupler is used to split the mixed signal comprising the public and stealth signals into two portions. To detect the BPSK signal, the portion in the public receiver is sent to a BPSK demodulator. As shown in Figure 13, the BPSK demodulator comprises a sine generator and a low-pass filter. The photocurrent of the BPSK public signal and the stealth signal during a 1-bit period can be respectively expressed as follows:

$$S_n(t) = \sqrt{\frac{2E_b}{T_b}} \cos\left[2\pi f_c t + \pi(1-b)\right], b = 0, 1, \tag{23}$$

$$S_{st}(t) = I_0 rect(t) = \begin{cases} I_0, 0 \le t \le T_b \\ 0, \quad other \end{cases}, \tag{24}$$

where E_b is the energy per bit, T_b is the 1-bit duration, f_c is the frequency of the carrier wave, b is the data, and I_0 is the intensity of the photocurrent. Then, the mixed photocurrent is multiplied by $\cos(2\pi f_c t)$, following which the photocurrent of the stealth signal can be written as

$$S_{st}(t) \cdot \cos(2\pi f_c t) = I_0 \cos(2\pi f_c t) \,. \tag{25}$$

Compared with Eqs. (13) and (14), the stealth signal contains the term cos($2\pi f_c t$). Because fc is much higher than the bit rate, the high-frequency terms are filtered out by the low-pass filter. Consequently, the public signal can be recovered successfully and relatively unaffected by the stealth signal.

To restore the stealth signal, the received signal is first passed through a CFBG, which is the same as that at the transmitter except with opposite dispersion. The stretched stealth signal is then compressed back to the original profile. At the decoder, the public BPSK signal is divided into mutually orthogonal SOPs with identical power by the PBS, which is designed according to the SOP of the CW laser. The power of the public signal from the upper and lower branches of the PBS is equal, as shown in Figure 14. For example, the electric field of the CW laser with linear +45 polarization is written as E(45°), and the PBS is designed to divide the light into two beams with horizontally linear polarization and vertically linear polarization. The electric fields of the two beams can be expressed as E(45°)cos45° and E(45°)sin45°. Next, the final subtraction after the photodiodes is given by

$$\mathrm{E}(45^{\circ})\cos 45^{\circ} - \mathrm{E}(45^{\circ})\sin 45^{\circ} = 0, \tag{26}$$

Thus, the public signal is eliminated by the double balance-difference detection. In the next section, we derive the signal-to-noise ratio (SNR) and bit-error rate (BER) to evaluate the system's performance.

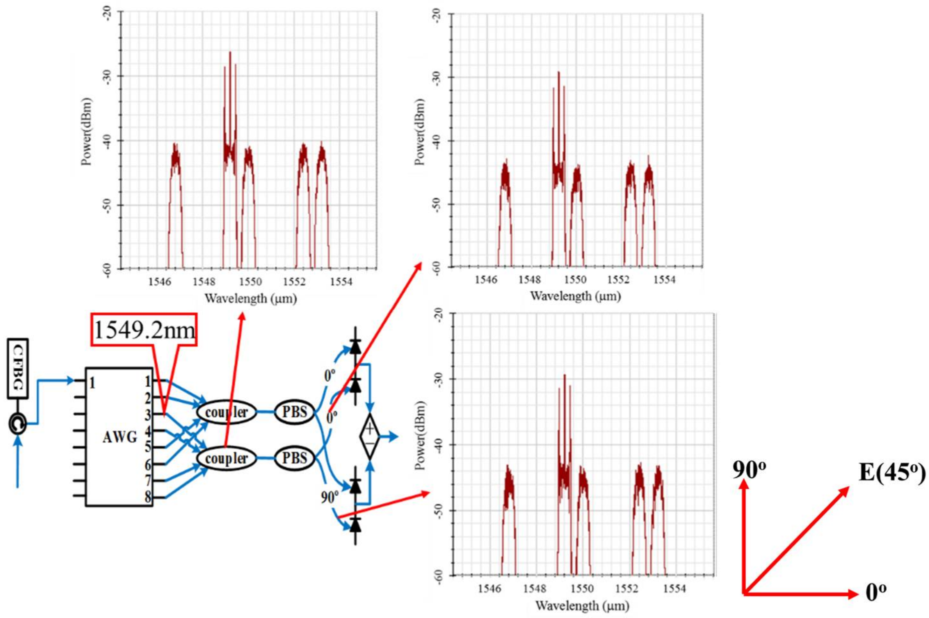


Figure 14. Public signal in decoder of stealth channel.

3.3. System performance with stealth signal

We assume that the broadband light source of the stealth channel is ideally unpolarized and its spectrum is flat in the bandwidth range [$\nu_0-\Delta\nu/2$, $\nu_0+\Delta\nu/2$], where ν_0 is the central optical frequency and $\Delta\nu$ is the optical source bandwidth. From the aforementioned assumptions, we can easily calculate the proposed system performance using Gaussian approximation and $u(v)$, the unit step function, which is expressed as

$$u(v) = \begin{cases} 1, & v \geq 0 \\ 0, & v < 0 \end{cases} . \tag{27}$$

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 21 August 2018 doi:10.20944/preprints201808.0367.v1

Peer-reviewed version available at *Appl. Sci.* **2018**, *8*, 1731; doi:10.3390/app8101731

Let $C_k(i)$ be the ith element of the kth low of the Walsh–Hadamard matrix. The power spectral density (PSD) of the received optical signal can be written as

$$s(v) = \frac{P_{sr}}{\Delta v}\sum_{i=1}^{N}[b_k c_k(i) + b_k \overline{c_k}(i)]rect(i)\,, \tag{28}$$

where P_{sr} is the effective power from a single source at the receiver, b_k is the data bit of the stealth signal, and N is the length of the codeword. The $rect(i)$ function in Eq. (28) is given by

$$rect(i) = u[v - v_0 - \frac{\Delta v}{2N}(-N+2i-2)] - u[v - v_0 - \frac{\Delta v}{2N}(-N+2i)]\,. \tag{29}$$

The PSD at PD_1, PD_2, PD_3, and PD_4 of the stealth receiver during the 1-bit period can be written as follows:

$$G_1(v) = \frac{P_{sr}}{\sqrt{2}\Delta v}\sum_{i=1}^{N} b_k[c_k(i)\cdot c_k(i)]\{rect(i)\}\,, \tag{30}$$

$$G_2(v) = \frac{P_{sr}}{\sqrt{2}\Delta v}\sum_{i=1}^{N} b_k[c_k(i)\cdot \overline{c_k}(i)]\{rect(i)\}\,, \tag{31}$$

$$G_3(v) = \frac{P_{sr}}{\sqrt{2}\Delta v}\sum_{i=1}^{N} b_k[\overline{c_k}(i)\cdot c_k(i)]\{rect(i)\}\,, \tag{32}$$

$$G_4(v) = \frac{P_{sr}}{\sqrt{2}\Delta v}\sum_{i=1}^{N} b_k[\overline{c_k}(i)\cdot \overline{c_k}(i)]\{rect(i)\}\,, \tag{33}$$

The coefficient $\sqrt{2}$ results from using a PBS. Using Eqs. (5) and (6), the detected photocurrent from the stealth signal at PD_1–PD_4 can be written as I_1, I_2, I_3, and I_4, respectively:

$$I_1 = R\int_0^{\infty} G_1(v)dv = \frac{RP_{sr}}{\sqrt{2}N}[b_k \frac{N}{2}]\,, \tag{34}$$

$$I_2 = R\int_0^{\infty} G_2(v)dv = 0\,, \tag{35}$$

$$I_3 = R\int_0^{\infty} G_3(v)dv = 0\,, \tag{36}$$

$$I_4 = R\int_0^{\infty} G_4(v)dv = \frac{RP_{sr}}{\sqrt{2}N}[b_k \frac{N}{2}]\,, \tag{37}$$

The signal from the stealth channel is given by the difference between the photodiode current outputs:

$$I_1 - I_2 = R\int_0^{\infty} G_1(v)dv - R\int_0^{\infty} G_2(v)dv = \frac{RP_{sr}}{\sqrt{2}N}[b_k \frac{N}{2}]\,, \tag{38}$$

$$I_3 - I_4 = R\int_0^{\infty} G_3(v)dv - R\int_0^{\infty} G_4(v)dv = -\frac{RP_{sr}}{\sqrt{2}N}[b_k \frac{N}{2}]\,. \tag{39}$$

After the second differential detection, the signal can be expressed as

$$I = (I_1 - I_2) - (I_3 - I_4) = \begin{cases} \frac{RP_{sr}}{\sqrt{2}}, & b_k = 1 \\ 0, & b_k = 0 \end{cases}\,. \tag{40}$$

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 21 August 2018 doi:10.20944/preprints201808.0367.v1

Peer-reviewed version available at Appl. Sci. 2018, 8, 1731; doi:10.3390/app8101731

Noise existing in the proposed SPC-OCDMA system comprises phase-induced intensity noise (PIIN), shot noise, thermal noise, and system noise in the public channel. The frequency band of the public noise is similar to that of the stealth noise. Public noise is difficult to eliminate using normal optical steganography. Using the duplicate process of public signal cancellation at the OCDMA decoder, public noise can be reduced because of white noise is unpolarized. Therefore, we use a factor α to denote the decrease in public noise. Using Eq. (40), we can obtain the variance of the photocurrent of noise as

$$\begin{aligned}\langle i^2\rangle &= \langle I^2_{shot}\rangle + \langle I^2_{PIIN}\rangle + \langle I^2_{thermal}\rangle + (\alpha I_{pn})^2 \\ &= 2eIB + 2I^2 B\tau_c + 4K_b T_n B / R_L + (\alpha I_{pn})^2 \quad , \\ &= 2e\left(\frac{RP_{sr}}{\sqrt{2}}\right)B + \frac{BR^2P^2_{sr}}{\Delta v} + \frac{4K_b T_n B}{R_L} + (\alpha I_{pn})^2\end{aligned} \tag{41}$$

where P_{sr} is the effective power from a single source at the receiver, R is the responsibility of PD, B is the noise-equivalent electrical bandwidth of the receiver, τ_c is the coherence time of the source, e is the electron charge, K_b is Boltzmann's constant, T_n is the absolute receiver noise temperature, and R_L is the receiver load resistor.

Using Eqs. (40) and (41), the SNR of the stealth signal can be represented as

$$SNR = \frac{\left(I_{b_k=1} - I_{b_k=0}\right)^2}{\langle I^2_{PIIN}\rangle + \langle I^2_{shot}\rangle + \langle I^2_{thermal}\rangle + (\alpha I_{pn})^2} = \frac{\left(\frac{RP_{sr}}{\sqrt{2}}\right)^2}{2e\left(\frac{RP_{sr}}{\sqrt{2}}\right)B + \frac{BR^2P^2_{sr}}{\Delta v} + \frac{4K_b T_n B}{R_L} + (\alpha I_{pn})^2} . \tag{42}$$

Based on an approximation to the Gaussian distribution, the BER of the SPC-OCDMA system can be expressed as

$$\text{BER} = \frac{1}{2} erfc\left[\left(\frac{SNR}{8}\right)^{\frac{1}{2}}\right], \tag{43}$$

where $erfc$ is the complementary error function, which can be expressed as

$$erfc = \frac{2}{\sqrt{\pi}}\int_x^{\infty} \exp(-t^2)dt . \tag{44}$$

Thus, we can draw BER-related curves using the aforementioned equations. When the public noise power is −3 dBm, the correlation between the BER and received stealth signal is as shown in Figure 15.

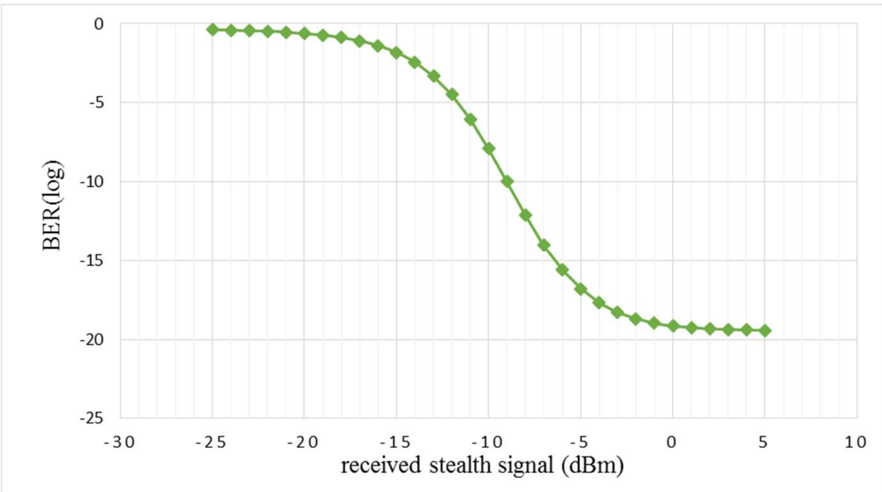


Figure 15. BER versus received stealth signal.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 21 August 2018 doi:10.20944/preprints201808.0367.v1

Peer-reviewed version available at Appl. Sci. 2018, 8, 1731; doi:10.3390/app8101731

The BER decreases with increasing power of the received stealth signal. A BER of 10^{-9} is achieved when the received power is −9 dBm.

Figure 16 shows the relationship between the received power of public noise and BER when the received power of the stealth SPC signal is −5, −10, −15, and −20 dBm.

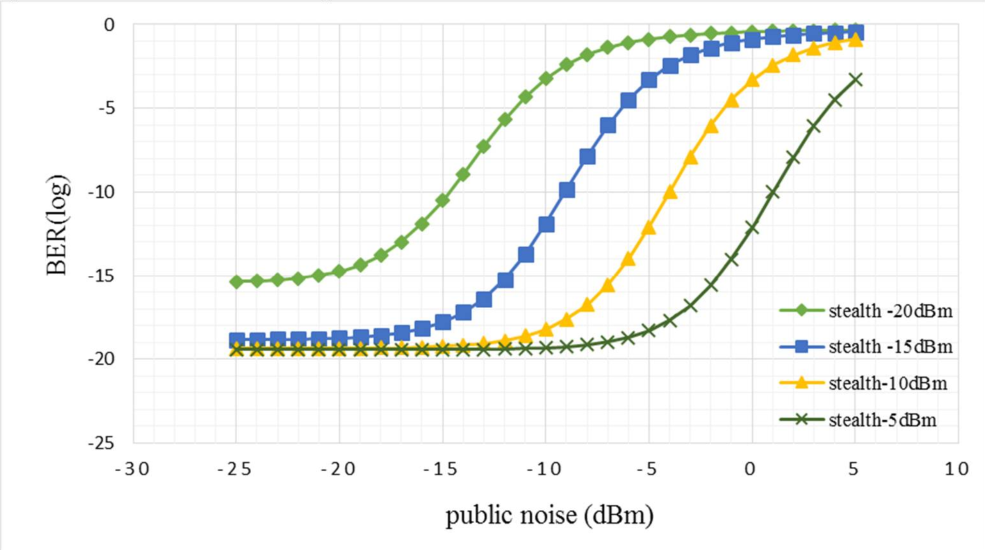


Figure 16. BER versus received power of public noise.

From Figure 16, we observe that the BER decreases when the received public noise power increases. The BER remains constant once the received public noise power has decreased to below a certain value. This is because the received public noise is neglected compared with the shot noise, thermal noise, or PIIN. The larger the power of the public noise, the more confidential the stealth signal. With larger public noise, the stealth signal can be hidden more efficiently, but this causes a higher BER. By contrast, smaller noise power results in superior BERs.

The relative parameters used in the analysis are shown in Table 1.

Table 1. Relative parameters used in BER analysis.

B **: noise-equivalent electrical bandwidth of the receiver**	0.5GHz
Kb **: Boltzmann's constant**	1.38×10^{-23} J/K
Tn **: absolute receiver noise temperature**	300K
$\boldsymbol{R_L}$**: receiver load resistor.**	1030Ω
Δ*v* **: optical source bandwidth**	1 THz
R **: responsibility of the PD**	0.8A/W
α :public noise-suppression factor	0.01

Next, power attenuation due to the free space optical link is calculated. The performance of the FSO system is affected most strongly by atmospheric turbulence. Although the influence of outer limits is unavoidable, we can control the internal parameters of the FSO system, such as the transmission power of the optical source, laser beam divergence, and receiver aperture area. Opti-System 7.0 is used to calculate the power attenuation. The system parameters are displayed in Table 2.

Table 2. Relative parameters employed for calculating power attenuation

L: range	1 km	
Ω: attenuation	3 dB/km (clear sky)	8dB/km (heavy rain)[22]
Dt: transmitter aperture diameter	4 cm	
Dr: receiver aperture diameter	8 cm	

θ: beam divergence	1 mrad

The power attenuation is observed to be −25 and −30 dB under weather conditions of clear sky and heavy rain, respectively. We discuss the correlation between the BER and transmission distance under the weather conditions of a clear sky and rainy day. The transmission power is set to 20 dBm, which is the maximum value that ensures eye and skin safety.

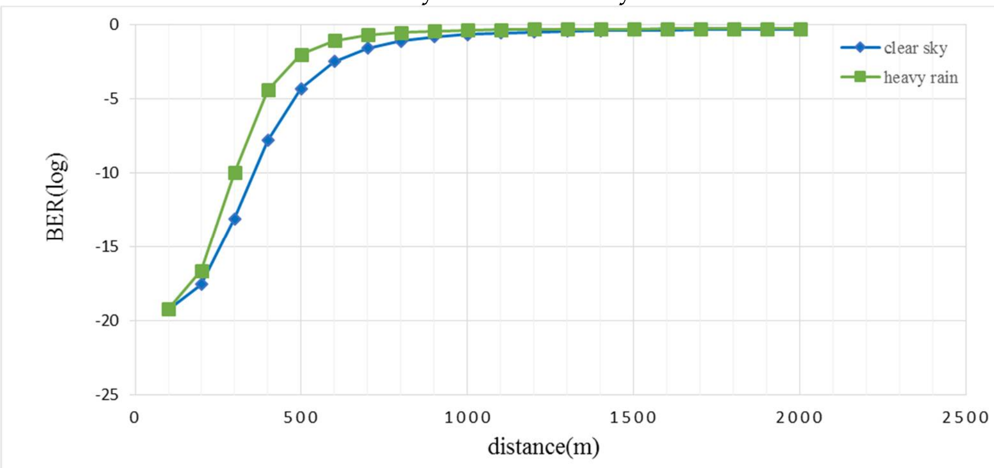


Figure 17. BER versus transmission distance.

The BER is found to increase as the transmission distance increases, and it is 2.4×10^{-9} when the transmission distance is 320 m on a rainy day. When the sky is clear, a BER of 1.62×10^{-9} is achieved at a transmission distance of 380 m.

5. Conclusions

The present study is preliminary research investigating the probability of applying other types of OCDMA in optical steganography. We have proposed a novel optical steganography transmission technique that conceals SPC-OCDMA signals in a public BPSK channel. A Walsh–Hadamard code is employed as a signature code for assigning a vertically or horizontally linear SOP to each specified wavelength. A CFBG provides considerable dispersion in a small size. The scale of the device is approximately 2000 times smaller compared with a single-mode fiber providing the same dispersion. Herein, the CFBG provides a dispersion of 1600 ps/nm and transforms the stealth signal into a noise-like signal so that it can be buried in the public channel.

The results indicate that the security of the system is enhanced because no one except the intended recipient knows the existence of the stealth signal in either the spectral or time domain. The power of the public noise is proportional to the security of the system and inversely proportional to the performance of the stealth channel. That is, with larger public noise, the stealth signal can be hidden more efficiently but the BER is higher. We propose 1-Gbps stealth transmission with a FSO link.

Furthermore, the pair of CFBGs adds another dimension to the key space of the stealth channel. An eavesdropper needs the correct dispersion compensator to detect the stealth signal. Even if the correct dispersion is obtained by using a tunable dispersion compensator, the eavesdropper cannot recover the data without the corresponding receiver.

The results show that the stealth signal is favorably hidden in the public channel and that our proposed optical steganography system provides high security when the average power of the stealth signal, public signal, and public noise are −5, 0, and −3 dBm, respectively. A range of FSO transmission of up to 380 m can be achieved at a BER of 1.62×10^{-9} under a clear sky and 320 m at a BER of 2.4×10^{-9} on a rainy day.

Acknowledgments: This study was supported in part by the Ministry of Science and Technology MOST 106-2622-E-150-018-CC3 and National Formosa University 106B096.

Author Contributions: Chih-Ta Yen performed the simulations and algorithm analysis, and contributed to a main part of manuscript writing. Jen-Fa Huang and Wen-Zong Zhang contributed in conceiving and the corresponding data analysis. All authors contributed to the writing of the paper.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Wu, B.; Shastri, B.J.; Mittal, P.; Tait, A.N.; Prucnal, P.R. Optical Signal Processing and Stealth Transmission for Privacy. *IEEE Journal of Selected Topics in Signal Processing* **2015**, *9*, 1185-1194, DOI: 10.1109/JSTSP.2015.2424690.
2. Zeng, G. *Quantum Private Communication*, 2010 edition; Springer: American, New York City, 2010.
3. Fok, M.P.: Prucnal, P.R. All-optical encryption for optical network with interleaved waveband switching modulation. Conference on Optical Fiber Communication 2009, San Diego, CA, USA. 22-26 March 2009.
4. Zhen, F.; PU, T.; Wei, Z.H.; Fang, T.; Chen, Y.F.; Zheng, J.L. Optical steganographic transmission of spectral-phase-encoded OCDMA signal over a public DPSK channel. 2013 22nd Wireless and Optical Communication Conference 2013, Chongqing, China, 16-18 May 2013.
5. Jamil, T. Steganography: the art of hiding information in plain sight. *IEEE Potentials* **1999**, *18*, 10-12, DOI: 10.1109/45.747237.
6. Channalli, S.; Jadhav, A. Steganography An Art of Hiding Data. *International Journal on Computer Science and Engineering* **2009**, *1*, 137-141, DOI: 10.3923/itj.2004.245.269.
7. Wu, B.; Narimanov, E. Secure stealth transmission over an existing public fiber-optical network. Optical Fiber Communication Conference and the National Fiber Optic Engineers Conference 2006, Anaheim, CA, USA, 5-10 March 2006.
8. Wu, B.; Narimanov, E. A method for secure communications over a public fiber-optical network. *Optics Express* **2006**,*14*, 3738-3751, DOI: 10.1364/OE.14.003738.
9. Kravtsov, K.; Wu, B.; Glesk, I.; Prucnal, P.R.; Narimanov, E. Stealth Transmission over a WDM Network with Detection Based on an All-Optical Thresholder. IEEE Lasers and Electro-Optics Society Annual Meeting Conference Proceedings 2007, Lake Buena Vista, FL, USA, 21-25 Oct. 2007.
10. Wu, B.; Agrawal, A.; Glesk, I.; Narimanov, E.; Etemad, S.; Prucnal, P.R. Steganographic fiber-optic transmission using coherent spectral phase-encoded optical CDMA. Conference on Lasers and Electro-Optics 2008, San Jose, CA, USA, 4-9 May 2008.
11. Wang, Z.; Prucnal, P.R. Optical Steganography Over a Public DPSK Channel With Asynchronous Detection. *IEEE Photonics Technology Letters* **2011**, *23*, 48-50, DOI: 10.1109/LPT.2010.2090516.
12. Wu, B.; Tait, A.N.; Chang, M.P.; Prucnal, P.R. WDM optical steganography based on amplified spontaneous emission noise. *Opt Lett* **2014**, *39*, 5925-5928, DOI: 10.1364/OL.39.005925.
13. Hong, X.; Wang, D.; Xu, L.; He, S. Demonstration of optical steganography transmissionusing temporal phase coded optical signals with spectral notch filtering. *Opt. Express* **2010**, *18*, 12415-12420, DOI: 10.1364/OE.18.012415.
14. Chen, Y.; Wang, R.; Fang, T.; Pu, T.; Xiang, P.; Zhu, H.; Zhang, J. Stealth transmission of temporal phase en/decoded polarization modulated code-shift-keying optical code division multiple access signal over synchronous digital hierarchy network with asynchronous detection. *Opt Eng* **2014**, *3*, 066103, DOI: 10.1117/1.OE.53.6.066103.
15. Zhu, H.; Wang, R.; Pu, T.; Chen, Y.; Fang, T.; Zheng, J.; Su, G. Complementary coding optical stealth transmission based on amplified spontaneous emission light source. *Opt. Express* **2014**, *22*, 28346-52, DOI: 10.1364/OE.22.028346.
16. Agrawal, G.P. Fiber-Optic Communications Systems. 3th ed.; Wiley, John & Sons, Incorporated, United States, New York City, 2002; pp. 38-42.
17. Huang, J.F.; Yang, C.C.; Tseng, S.P. Complementary Walsh–Hadamard coded optical CDMA coder/decoders structured over arrayed-waveguide grating routers. *Optics Communications* **2004**, *229*, 241-248, DOI: 10.1016/j.optcom.2003.11.007.
18. Yen, C.T.; Cheng, H.C.; Chang, Y.T.; Chen, W.B. Performance Analysis of Dual Unipolar/Bipolar Spectral Code in Optical CDMA Systems. *Journal of Applied Research and Technology* **2013**, *11*, 235-241, https://doi.org/10.1016/S1665-6423(13)71533-5.
19. Wang, C.; Yao, J. Fiber Bragg gratings for microwave photonics subsystems. *Opt Express* **2013** *21* 22868-22884, DOI: 10.1364/OE.21.022868.

Peer-reviewed version available at *Appl. Sci.* **2018**, *8*, 1731; doi:10.3390/app8101731

20. Fok, M.P.; Prucnal, P.R. Optical Steganography Using Chirped Fiber Bragg Grating. Optical Fiber Communication Conference and National Fiber Optic Engineers Conference 2009, San Diego, CA, USA, 22-26 March 2009.
21. Malik, A.; Singh, P. Free Space Optics: Current Applications and Future Challenges. *International Journal of Optics* **2015**, *2015*, 1-8, http://dx.doi.org/10.1155/2015/945483.
22. Sahbudin, R.K.Z.; Kamarulzaman, M.; Hitam, S.; Mokhtar, M.; Anas, S.B.A. Performance of SAC OCDMA-FSO communication systems. *Optik* **2013**, *124*, 2868–2870, DOI: 10.1016/j.ijleo.2012.08.067.