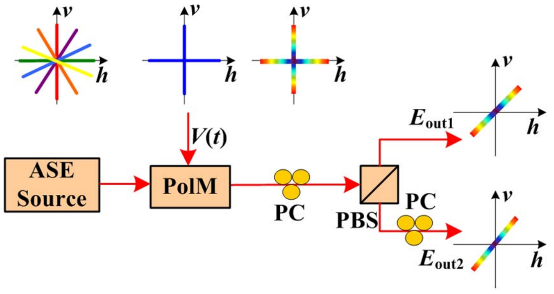
IEEE Photonics Journal
An IEEE Photonics Society Publication

Optical Steganography of Code-Shift-Keying OCDMA Signal Based on Incoherent Light Source

Volume 7, Number 3, June 2015

Huatao Zhu, Student Member, IEEE
Rong Wang
Tao Pu, Member, IEEE
Tao Fang
Peng Xiang
Jilin Zheng
Weijiang Wu



DOI: 10.1109/JPHOT.2015.2432072
1943-0655 © 2015 IEEE

Optical Steganography of Code-Shift-Keying OCDMA Signal Based on Incoherent Light Source

Huatao Zhu, *Student Member, IEEE*, Rong Wang, Tao Pu, *Member, IEEE*, Tao Fang, Peng Xiang, Jilin Zheng, and Weijiang Wu

College of Communications Engineering, PLA University of Science and Technology,
Nanjing 210007, China

DOI: 10.1109/JPHOT.2015.2432072

Manuscript received March 10, 2015; revised May 5, 2015; accepted May 7, 2015. Date of publication May 12, 2015; date of current version May 27, 2015. This work was supported in part by the National Natural Science Foundation of China under Grant 61475193, Grant 61177065, and Grant 61174199 and in part by Jiangsu Province Science Foundation Council under Grant BK20140069. All authors contributed equally to this work. Corresponding author: T. Pu (e-mail: nj_putao@163.com).

Abstract: In this paper, a method to enhance the security of the optical stealth channel is proposed. The proposed method uses the techniques of polarization modulator based code-shift-keying (CSK) data modulation and optical code-division multiple-access (OCDMA) en/decoding, where an incoherent light source is needed. Our analysis and experimental results show that the CSK-OCDMA signal, where a wavelength selective switch is used for optical en/decoding, has been stealthily transmitted over a 40-km wavelength-division multiplexing optical fiber link. In addition, the stealth channel only causes a power penalty less than 0.48 dB to the public channel, whereas both of these two channels can achieve error-free transmission (with bit error rate less than 10^{-9}).

Index Terms: Optical code-division multiple access (OCDMA), optical steganography, optical security and encryption, code-shift keying (CSK).

1. Introduction

The enhancement of information security in the physical layer of modern optical networks is becoming an important issue that is drawing much attention in the research of optical networking. Many approaches have been studied, such as quantum secure communication [1], [2], optical chaotic encryption [3], [4], and optical code division multiple access (OCDMA) [5]–[8]. Both optical chaotic encryption and OCDMA can encode the transmitted data as noise-like signals, and the two technologies can be used to hide the secure signal under the background noise of public network. Dissimilar to the optical steganography based on optical chaotic encryption, OCDMA based optical stealth system does not require the synchronization between transmitter and receiver. In OCDMA based optical steganography, optical pulses are encoded into noise-like signals with a very low average power (even below the system noise floor) by coherent OCDMA encoders. Thus, the stealth transmission of information is achieved by inserting this OCDMA channel into an existing public channel. Based on this principle, some coherent OCDMA based optical steganography experimental systems have been demonstrated [9]–[13]. However, the optical spectrum of the stealth signal is narrow compared with the system noise. Recently, the method of optical steganography using the amplified spontaneous emission (ASE) noise as the

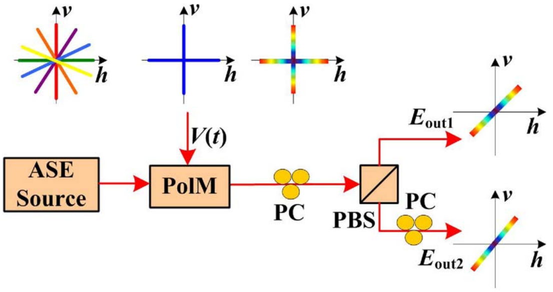


Fig. 1. Schematic of CSK modulation for incoherent light. PC: Polarization controller.

carrier for stealth channel has been proposed [14], [15]. The ASE noise have the same characteristic as the system noise, therefore, the stealth signal carried by ASE noise can hide under a public channel well both in frequency and time domain [15].

In this paper, we demonstrate the code-shift keying (CSK) modulation based on polarization of incoherent light source. Then, a proof-of-concept experiment is carried out to demonstrate the security enhancement of the stealth channel based on OCDMA signal by combing the CSK modulation and optical en/decoding with the incoherent light, which is generated by an ASE source. In the stealth channel, we use wavelength selective switch (WSS) as the OCDMA en/decoder, which provides a reconfiguration solution. This paper is organized in the following matter. In the second section, the principle and experiment setup of the proposed system is introduced. In the third section, the experimental results and discussions are provided. Then, the conclusions are drawn in the final section.

2. Principle

Fig. 1 shows the schematic diagram illustrating the generation of CSK-OCDMA signals. The optical signals from the ASE light source, which has a random polarization state, is phase modulated by the polarization modulator (PolM) along its horizontal and vertical principal axes. The normalized optical field of the output signals from the PolM output can be expressed as

$$\begin{bmatrix} E_h \\ E_v \end{bmatrix} = \frac{\sqrt{2}}{2} E_0 \begin{bmatrix} \exp\left(j\omega t + \frac{j\pi V(t)}{V_\pi}\right) \\ \exp\left(j\omega t - \frac{j\pi V(t)}{V_\pi}\right) \end{bmatrix} \tag{1}$$

where E_0 is the amplitude of ASE signal optical field, ω is the angular frequency of ASE signal, $V(t)$ is the microwave drive signal, and V_π is the half-wave voltage of the PolM. By adjusting the polarization controller, the polarization beam splitter (PBS) has polarization angles of $\pi/4$ and $3\pi/4$ to the two principal axes of the PolM respectively. The two outputs of the PBS can be expressed as

$$E_{\text{out1}} = \frac{\sqrt{2}}{2}(E_h + E_v) = E_0 \cos\left[\frac{\pi V(t)}{V_\pi}\right] \exp(j\omega t) \tag{2}$$

$$E_{\text{out2}} = \frac{\sqrt{2}}{2}(E_v - E_h) = E_0 \sin\left[\frac{\pi V(t)}{V_\pi}\right] \exp(j\omega t) \tag{3}$$

where $V(t)$ is a the non-return to zero square wave whose amplitude is $V_\pi/2$. Therefore, the 0 bits and 1 bits go to the two different outputs of the PBS, and they are encoded by two WSS, respectively. Then, the two outputs are combined by an optical coupler to generate stealth CSK-OCDMA signal. A polarization controller is used to equalize the polarization of signal in the two paths.

The schematic diagram of the stealth transmission system is shown in Fig. 2. At the transmitter side, a continue-wave (CW) laser module is used to generate the public signal at 2.5 Gb/s with 2^{15}–1 pseudo-random binary sequence (PRBS). The center wavelength of the CW laser

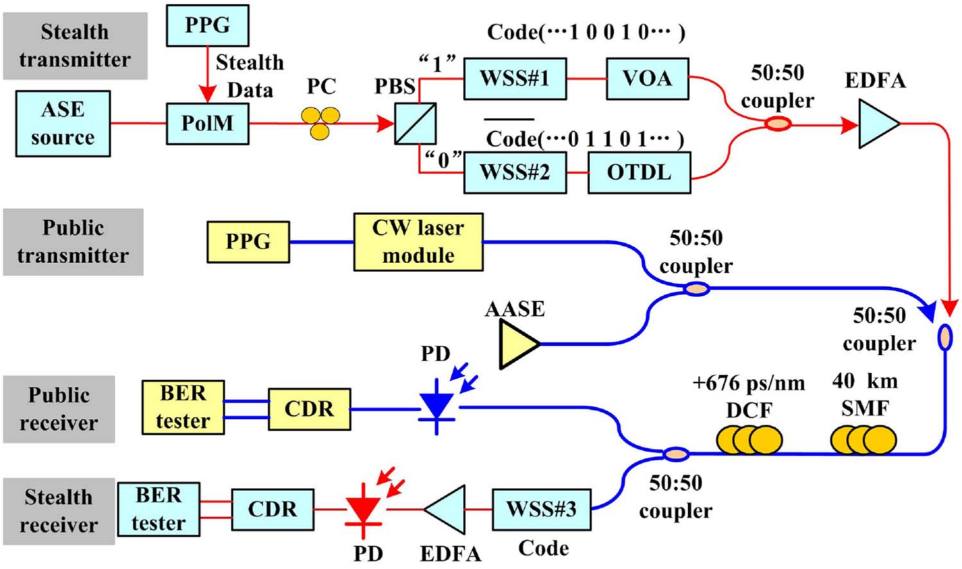


Fig. 2. Schematic diagram of CSK-OCDMA based optical stealth transmission system. PPG: programmable pulse generator; AASE: additional amplified spontaneous emission; BER: bit error rate; PD: photonic detector.

module is set as 1551.82 nm, and the 20-dB bandwidth is 0.3 nm. A PolM and a PBS are used to modulate the light beam from ASE light source at 2.5 Gb/s with 2^7–1 PRBS to generate the CSK signal. The center wavelength of the ASE light source is 1546.4 nm and 20-dB bandwidth is 45.3 nm. Following the two ports of PBS, two WSS are used for optical encoding. The WSS with channel space complying the 50 GHz ITU-T grid is used, which can reconfigure the codes in less than 500 ms. The equalization of power and the synchronization between the two ports are required in order to keep the characteristic of stealth CSK-OCDMA signal unchanged compared with the signal from the ASE light source in time and spectral domain. Thus, an optical tunable delay line (OTDL) and a variable optical attenuation (VOA) are used. A 50:50 coupler is used to combine the signal from two parts. In addition, a polarization controller (PC) is added following the VOA to control the polarization of one part and keep its polarization parallel with the other part at the output of the coupler. To simulate the noise in optical networks, an additional ASE light source is added. The stealth CSK-OCDMA signal is injected into the public channel via another 50:50 optical coupler. Then, the combined signals are sent though a 40 km single mode fiber (SMF) span.

At the receiver side, to detect the combined signals, a dispersion compensation fiber (DCF) with dispersion of $+676$ ps/nm is used to compensate the fiber transmission dispersion. And then a 50:50 coupler splits the signals into two paths to detect the public signal and the stealth CSK-OCDMA signal respectively. For public channel, the energy detector followed by a clock and data recovery (CDR) module is used. For stealth channel, a WSS (WSS#3) is used to decode the stealth CSK-OCDMA signal and eliminate the public signal. The WSS#3 used in the receiver side has a matching code pattern with the WSS#1 in the transmitter; meanwhile, it can cut off the wavelength carrying the public channel functioning as a notch filter. In addition, an Erbium doped fiber amplifier (EDFA) followed by energy detector and CDR is used and the output power of the EDFA is -0.1 dBm. To test the transmission performance of each channel, bit error rate (BER) tester is used. The clock and data signals can be recovered by the CDR for each channel, without clock signals transmission.

The measured waveform of the CSK-OCDMA signal is shown in Fig. 3, where Fig. 3(a) and (b) show the signals from the two outputs of the PBS respectively. Fig. 3(c) is the original signal from the ASE light source, Fig. 3(d) is the combined signal and they are indistinguishable from each other. After splitting and combing, the stealth signal keeps its time domain characteristic.

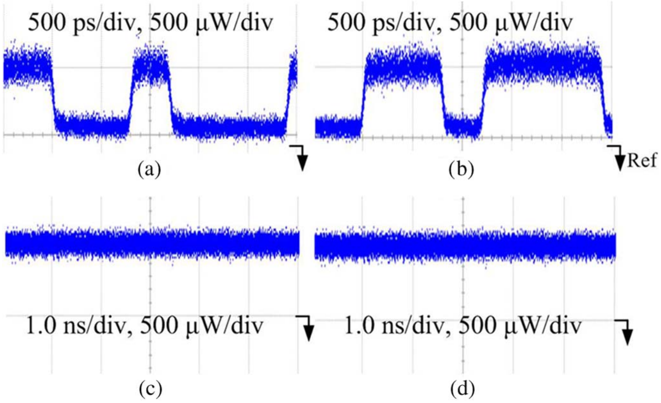


Fig. 3. Waveform diagrams of stealth signal. (a) Signal at one port of PBS. (b) Signal at the other port of PBS. (c) Signal from ASE light source. (d) Combined signal. Div: division. Ref: reference level.

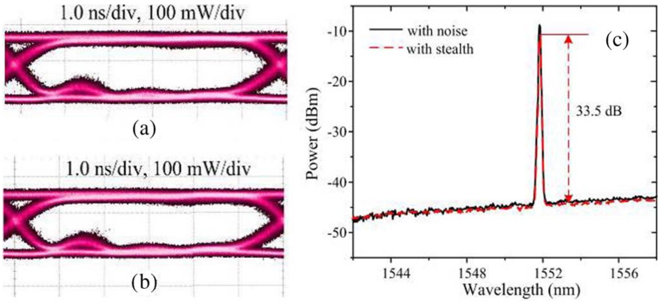


Fig. 4. Eye diagrams of public channel without (a) and with (b) stealth CSK-OCDMA signal. (c) Spectra of public channel.

Here, the modified Gold-code is used as the codes. An additional 0 bit is inserted at the end of the code sequence to equalize the number of the 0 bits and 1 bits. For instance, a code sequence with length of 15 is “1 1 1 1 0 1 0 1 1 0 0 1 0 0 0,” while the modified sequence is “1 1 1 1 0 1 0 1 1 0 0 1 0 0 0 0.” The modified code sequence can be easily generated by two m-sequences under the control of a synchronizing clock. The modified Gold-code has the same code space to the Gold-code. For instance, the code space of modified Gold-code with length of 64 is 64. In the experiment, due to the lack of enough WSS, two fixed band pass filters are used to replace the WSS at the transmitter side for optical encoding. For one filter, its center wavelength is 1550.35 nm and its 20-dB bandwidth is 21.2 nm. For another, its center wavelength is 1569.35 nm and its 20-dB bandwidth is 20.6 nm. If the WSS is available, it can reconfigure the codes in less than 500 ms.

3. Results and Discussion

3.1. Security Performance

In the experiment, the stealth CSK-OCDMA signal can be concealed well under the public channel both in the time domain and the spectral domain. When the average power ratio (ΔP) of the public channel and stealth channel is 12.0 dB, the eye diagram of the detected signal from the public channel without and with the stealth CSK-OCDMA signal is shown in Fig. 4(a) and (b) respectively. As can be seen, the two eye diagrams are indistinguishable. Thus, the stealth CSK-OCDMA signal has been temporally concealed in public channel. The spectra of the public channel with noise or stealth CSK-OCDMA signal is shown in Fig. 4(c). As can be

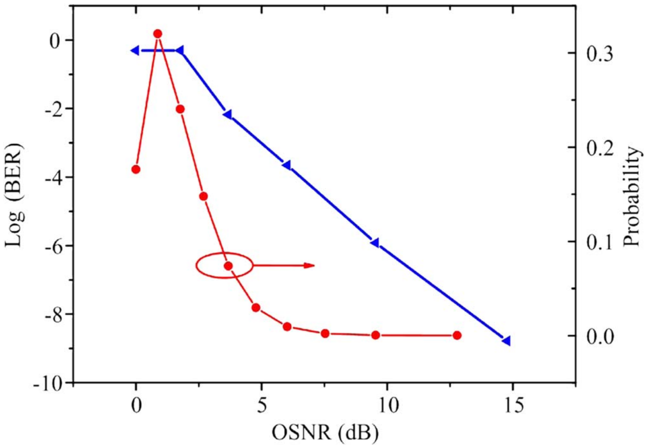


Fig. 5. Minimum BER and probability versus OSNR.

seen, the resemblance of two spectra indicates that the stealth CSK-OCDMA signal has also been concealed in public channel in the spectral domain. The power ratio of the peak of the public channel and that of the stealth signal is about 33.5 dB.

The stealth CSK-OCDMA signal has an identical temporal and spectral feature to the noise. Compared with the coherent OCDMA based optical steganography, the proposed CSK-OCDMA can be hidden under the public channel better. Therefore, the security of optical steganography has been enhanced.

For the case that the eavesdropper suppose there is a stealth channel under public channel. And the eavesdropper uses the same WSS to filter out the public signal and attack the stealth signal. When the number of filtered wavelength channels is x (x is no more than 96), the probability that y (y is no more than 48 and x) channels of them are 1 bits can be defined as

$$P = \left(\frac{1}{2}\right)^{x} \binom{y}{x}. \tag{4}$$

Let s be the average optical power of the eavesdropped stealth signal in a single wavelength channel, n_p the optical power of residual public signal, and n_n the optical power of the AASE noise. The stealth channel optical signal-to-noise ratio at the eavesdropper's receiver is defined as

$$\text{OSNR} = \begin{cases} \frac{xs}{(x-y)s+n_p+n_n}, & x \geq y/2 \\ \frac{(x-y)s}{ys+n_p+n_n}, & x < y/2. \end{cases} \tag{5}$$

Without the AASE noise, the measured minimum BER versus the OSNR is shown in Fig. 5 when x is 20. The BER is more than 10^{-4} while the OSNR is less than 5 dB. The probability versus OSNR is also shown in Fig. 5. The probability of the BER being more than 10^{-4} is 0.0026. The intercept probability is low. With the impact by noise in the public channel, the intercept probability will decrease.

3.2. Transmission Performance

For stealth channel, with the correct decoding at the receiver side and effective elimination of the public signal, the stealth signal can be recovered. The waveform and eye diagram of recovered stealth signal is shown in Fig. 6.

The measured results of BER for stealth channel are shown in Fig. 7(a). The scattered points are the measured results and the lines are linear regression results. Error-free transmission has been achieved for stealth channel when the ΔP of public channel and stealth channel is not less than 14.0 dB. Meanwhile, forward error correction (FEC) technology can be used to reduce

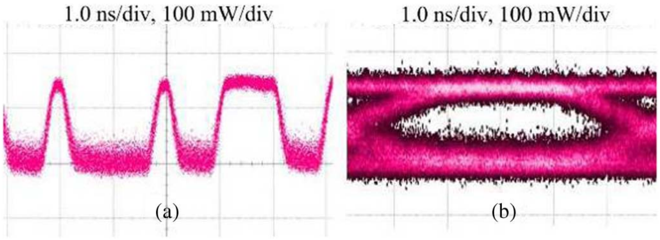


Fig. 6. Waveform (a) and eye diagram (b) for stealth channel at the receiver side.

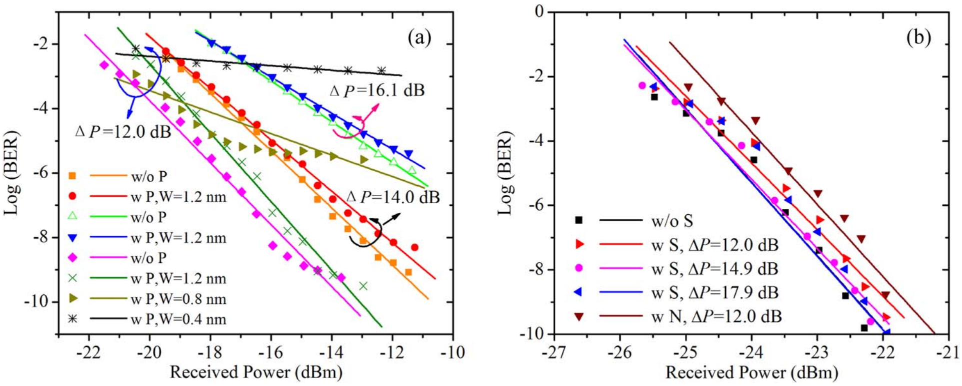


Fig. 7. (a) BER measurements of the stealth channel. (b) BER measurements of the public channel. W: with; w/o: without; P: public; S: stealth; N: noise; W: bandwidth of the notching.

the BER of 7.5×10^{-4} to be error-free [16]. As the ΔP increases, the BER of stealth channel increases as well. When the bandwidth of the notching is 1.2 nm and the central wavelength is 1551.72 nm, the public channel results in power penalty of 0.48 dB and 0.87 dB at ΔP of 12.0 dB and 14.0 dB respectively. As bandwidth of the notching decreases, the BER of the stealth channel increases on the contrary. When the bandwidth of the notching is 0.4 nm and central wavelength is 1551.72 nm, the notching missed to remove the entire public signal and the BER increases to about 10^{-3}. It is because the public signal has a 0.1 nm central wavelength larger than this notching and the short wavelength component can be eliminated effectively while the long wavelength component combines with the stealth channel. A WSS with 12.5 GHz ITU-T grid can be used to eliminate the public signal accurately.

Furthermore, if the proposed scheme is working in a multiple wavelength public channel, such as in the existing 100 GHz ITU-T grid wavelength division multiplexing (WDM) network, this scheme can also be available. The WSS#3 shuts down the channels matched with the multiple wavelength public signals at the receiver side and the residual channels can be used to decode and retrieve the stealth signal. And the FEC technology could be introduced to enhance the transmission performance of stealth channel.

Fig. 7(b) shows the measured results of the public channel. When ΔP of public channel and stealth channel is 17.9 dB, the stealth channel causes zero power penalty to the public channel. As the ΔP goes down, the power penalties go up oppositely. The stealth signal introduces 0.48 dB power penalty to public channel for $\Delta P = 12.0$ dB, while the noise results in 0.75 dB power penalty for that ΔP.

For the concern of privacy, the stealth channel should influence the public channel as little as possible, and the average power of the stealth signal should be low. However, in terms of the availability for stealth channel, the low-power stealth signal degrades the transmission performance of stealth channel. A compromise should be reached between the public channel and the stealth channel.

4. Conclusion

We propose and demonstrate polarization based code-shift keying modulation for incoherent light and utilize it with optical en/decoding in optical steganography to improve the security of the stealth signal in the optical stealth transmission system. The stealth signal is effectively hidden under the WDM channel during 40 km SMF transmission in both the spectral and the time domain and received with error-free performance at the receiver side. The stealth channel results in little interference to public channel. The proposed technique provides a potential application to the secure optical communication over the existing WDM network.

Acknowledgment

The authors would like to thank Prof. Shuwen Yang and Prof. Jianhua Ji for their help on the experimental device. The authors are also obliged to the reviewers for the careful review and helpful comments.

References

[1] E. Waks *et al.*, “Secure communication: Quantum cryptography with a photon turnstile,” *Nature*, vol. 420, no. 6917, pp. 762–762, Dec. 2002.

[2] W. Y. Hwang, “Quantum key distribution with high loss: Toward global secure communication,” *Phys. Rev. Lett.*, vol. 91, no. 5, Art. ID. 057901, Aug. 2003.

[3] G. D. VanWiggeren and R. Roy, “Communication with chaotic lasers,” *Science*, vol. 279, no. 20, pp. 1198–1200, Feb. 1998.

[4] P. M. Alsing, A. Gavrielides, V. Kovanis, R. Roy, and K. S. Thornburg, “Encoding and decoding messages with chaotic lasers,” *Phys. Rev. E, Stat. Nonlin. Soft Matter Phys.*, vol. 56, no. 6, pp. 6302–6310, Dec. 1997.

[5] A. Stock and E. H. Sargent, “The role of optical CDMA in access networks,” *IEEE Commun. Mag.*, vol. 40, no. 9, pp. 83–87, Sep. 2002.

[6] T. H. Shake, “Security performance of optical CDMA against eavesdropping,” *J. Lightw. Technol.*, vol. 23, no. 2, pp. 655–670, Feb. 2005.

[7] M. Liu, Y. Hsu, and J. Jiang, “Utilization of LDPC code and optical hard-limiter in OCDMA communication systems,” *IEEE Photon. J.*, vol. 6, no. 5, Oct. 2014, Art. ID. 7903311.

[8] S. A. Khan and J. Bajcsy, “Chip-asynchronous binary optical CDMA: An optimum signaling scheme for random delays,” *IEEE Photon. J.*, vol. 5, no. 2, Apr. 2013, Art. ID. 7200408.

[9] B. B. Wu, P. R. Prucnal, and E. E. Narimanovr, “Secure transmission over an existing public WDM lightwave network,” *IEEE Photon. Technol. Lett.*, vol. 18, no. 17, pp. 1870–1872, Sep. 2006.

[10] B. B. Wu and E. E. Narimanov, “A method for secure communications over a public fiber-optical network,” *Opt. Exp.*, vol. 14, no. 9, pp. 3738–3751, May 2006.

[11] X. Hong, D. Wang, L. Xu, and S. He, “Demonstration of optical steganography transmission using temporal phase coded optical signals with spectral notch filtering” *Opt. Exp.*, vol. 18, no. 12, pp. 12415–12420, May 2010.

[12] Z. Gao, X. Wang, N. Kataoka, and N. Wada, “Stealth transmission of time-domain spectral phase encoded OCDMA signal over WDM network” *IEEE Photon. Technol. Lett.*, vol. 22, no. 13, pp. 993–995, Jul. 2010.

[13] Y. Chen *et al.*, “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.*, vol. 53, no. 6, Jun. 2014, Art. ID. 066103.

[14] B. Wu *et al.*, “Optical steganography based on amplified spontaneous emission noise,” *Opt. Exp.*, vol. 21 no. 2, pp. 2065–2071, Jan. 2013.

[15] H. Zhu *et al.*, “Complementary coding optical stealth transmission based on amplified spontaneous emission light source,” *Opt. Exp.*, vol. 22, no. 23, pp. 28346–28352, Nov. 2014.

[16] B. Wu *et al.*, “Analog noise protected optical encryption with two-dimensional key space,” *Opt. Exp.*, vol. 22, no. 12, pp. 14568–14574, Jun. 2014.