Optical Steganography Communication Using Signal-carrying Noise Dispersion

Philip Y. Ma, Ben Wu, Bhavin J. Shastri, and Paul R. Prucnal
*Lightwave Communications Laboratory, Department of Electrical Engineering,
Princeton University, Princeton NJ, 08544, USA*
yechim@princeton.edu

Abstract: We propose an optical steganography approach that can be easily implemented in the existing communication networks. Chirped fiber Bragg grating (CFBG) is used to create the stealth communication channel and disperse the signal carried by amplified spontaneous emission (ASE) noise.

1. Introduction

Optical steganography is a method for hiding (stealth) signals in public fiber-optic communication channels. The initial approach employed long fiber spools and wide spectrum mode-locked laser (MLL) to hide the stealth signal in both the time and spectral domains [1]. Later on, a stealth communication channel was demonstrated to be established using widely existing amplified spontaneous emission (ASE) noise [2]. The usage of ASE noise reduces the implementation complexity and enables the possibility of multi-channel steganographic communication [3]. The problem is that phase modulation has to be used with an interferometer structure for homodyne detection, rendering the communication channel to be highly unstable due to temperature and mechanical vibrations. Without extra stability unit, new steganographic channel design is needed to make this technology more deployable in today's optical networks.

In this paper, we propose an optical steganography scheme where chirped fiber Bragg grating (CFBG) is used in conjunction with ASE noise. CFBG is able to not only achieve strong dispersion effect within an extremely short range [4], but also makes the system design become significantly compact and reliable. CFBG plays three important roles; it acts as: 1) a band-pass filter that allocates part of the ASE noise spectrum as the stealth channel optical source; 2) a stretcher that disperses the signal-carrying ASE noise even below the pure ASE noise level; 3) a corresponding compressor that is able to reshape the signal-carrying ASE noise if placed in the opposite orientation. Apart from its simplicity and reliability, this scheme also guarantees communication security as corroborated by spectrum analysis in the spectral domain and eye diagram measurements in the time domain.

2. Experimental setup

The experimental setup is shown in Fig. 1. Mach-Zehnder Modulator (MZM) is utilized for intensity modulating both the public and stealth data using pseudo-random bit sequence (PRBS). PRBS length is $2^{31}-1$ with a bit rate of 2.5 Gb/s. The public channel carrier is produced by a distributed feedback (DFB) laser source with a center wavelength of 1550.32 nm. An erbium doped fiber amplifier (EDFA1) amplifies the public signal and generates ASE noise into the channel. CFBG1 reflects back a small portion of the ASE noise band (∼0.9 nm with a central wavelength around 1530 nm) as the the stealth channel optical source. The rest of the ASE noise spectrum plus the public channel passes

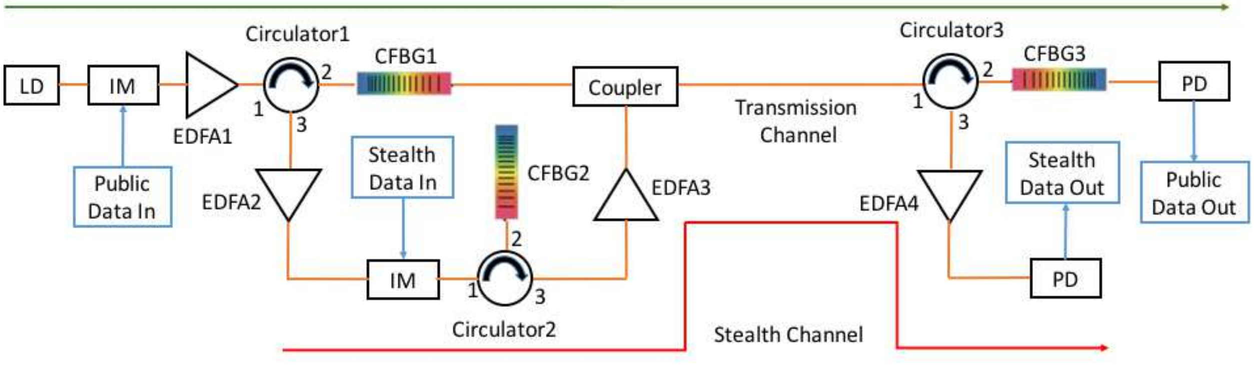

Fig. 1: Experimental setup of optical steganography (LD: laser diode, IM: intensity modulator, EDFA: erbium doped fiber amplifier, CFBG: chirped fiber Bragg grating, PD: photodiode).

978-1-5090-1906-9/16/$31.00 ©2016 IEEE

through CFBG1 without being affected. EDFA2 boosts the stealth channel power while CFBG2 disperses the stealth signal carried by ASE noise (the dispersion parameter is 1017 ps/nm). EDFA3 is used to compensate the power loss after passing through CFBG2. The public and stealth signals are combined at the coupler and transmitted together through the transmission channel where it is assumed to be susceptible to eavesdropping. CFBG3 not only separates the public and stealth channels, but also recovers the stealth signal by being placed in opposite orientation against CFBG1 and CFBG2. Direct detection using photodiode (PD) is employed at both the public and stealth receivers. EDFA4 is used to compensate the power loss after passing through CFBG3.

3. Results and discussion

We first perform the spectrum analysis of our optical steganography scheme (Fig. 2(a)-(d)). Fig. 2(a) shows the spectrum before splitting into two channels, which corresponds to a public channel peak with ASE noise background. Fig. 2(b) is the public channel spectrum after a narrow ASE noise band around 1530 nm being filtered out by CFBG1 as the stealth channel optical source. Fig. 2(c) is the stealth channel spectrum, exhibiting a power surge around 1530 nm that matches with the absence of this band in Fig. 2(b). Fig. 2(c) has an ASE noise background due to the fact that this spectrum is taken after EDFA3. Fig. 2(d) is the transmission channel spectrum after coupling both the public and stealth channels, which is identical to Fig. 2(a) with the only difference that stealth signal has been added. We also perform the analysis in the time domain with the aid of eye diagram measurements (Fig. 2(e)-(h)). Fig. 2(e) shows the public signal while Fig. 2(f) shows the stealth signal after being dispersed by CFBG2 which looks like pure ASE noise. The transmission channel eye diagram shown in Fig. (g) further verifies that the stealth signal only contributes to the noise level of public signal. The amplification factor of EDFA3 can be tuned so that the stealth channel power remains constant with or without stealth data modulation. In that case, the transmission channel eye diagram will not change with or without stealth channel. Fig. 2(i) is the stealth signal successfully recovered by CFBG3.

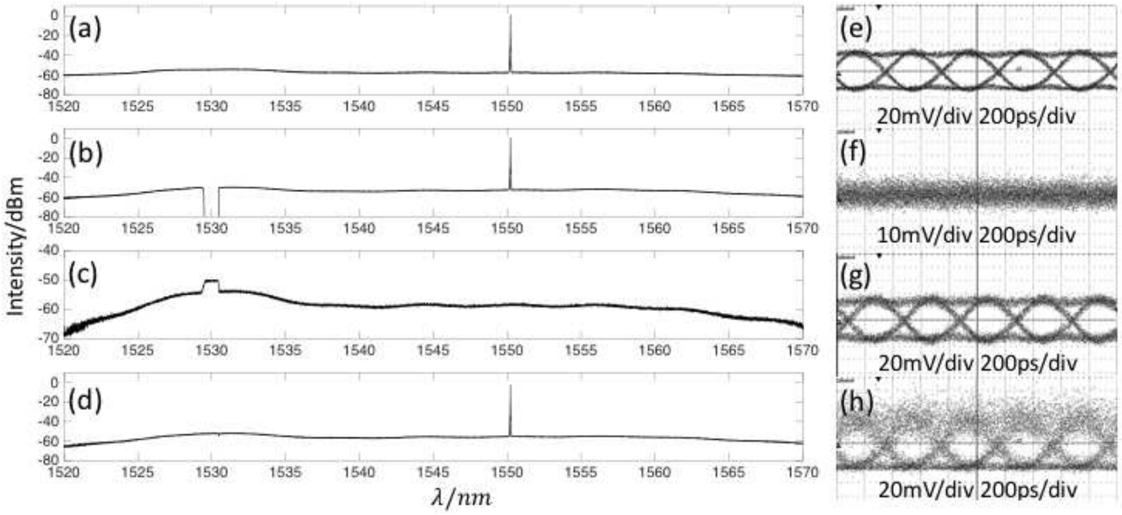

Fig. 2: Left: Frequency spectra (a) before CFBG1, (b) of public channel, (c) of stealth channel, (d) of transmission channel. Right: Eye diagrams of (e) public signal, (f) stealth signal after being dispersed by CFBG2, (g) transmission channel signal with both public and stealth signal, (h) stealth signal after being recovered by CFBG3.

4. Conclusion

We demonstrated an optical steganography scheme using ASE noise and CFBG. The implementation is simplified and the stealth channel security is ensured in both the time and spectral domains. Future research involves measurements of bit error rate (BER) and investigation of mutual channel influence.

References

1. B. Wu, A. Agrawal, I. Glesk, E. Narimanov, S. Etemad, and P. Prucnal, ”Steganographic fiber-optic transmission using coherent spectral-phase-encoded optical CDMA,” CFF5, CLEO (2008).
2. B. Wu, Z. Wang, Y. Tian, M. P. Fok, B. J. Shastri, D. R. Kanoff, and P. R. Prucnal, ”Optical steganography based on amplified spontaneous emission noise,” Opt. Express **21**, 2065-2071 (2013).
3. B. Wu, A. N. Tait, M. P. Chang, and P. R. Prucnal, ”WDM optical steganography based on amplified spontaneous emission noise,” Opt. Lett. **39**, 5925–5928 (2014) .
4. M. P. Fok and P. R. Prucnal, ”A Compact and Low-Latency Scheme for Optical Steganography Using Chirped Fiber Bragg Gratings,” Electron. Lett. **45**, 179–180 (2009).