Steganographic Communication via Spread Optical Noise: A Link-Level Eavesdropping Resilient System

Philip Y. Ma, *Student Member, IEEE*, Ben Wu, Bhavin J. Shastri, Alexander N. Tait, *Member, OSA*,
Prateek Mittal, *Member, IEEE*, and Paul R. Prucnal, *Fellow, IEEE, Fellow, OSA*

Abstract**—**[illegible]

limited by their low throughput and considerable coding overhead [35].

In the context of optical communication, *optical steganography* was proposed as a form of analog steganography to enable steganographic communication over optical transmission channels that can be publicly accessed by eavesdroppers [36]. These initial schemes, using either the conventional long-distance fiber spool [37]–[39], or chirped fiber Bragg grating (CFBG) [40]–[42], spread the stealth signal in the time domain to reduce its power level below the noise. In order to conceal the existence of the low power stealth signal in the frequency domain, additional high power public (cover) signal has to co-exist at the same channel bandwidth, which not only restricts their practical usage in real optical networks where bandwidth resources are limited, but also requires [illegible] delicate channel separation techniques

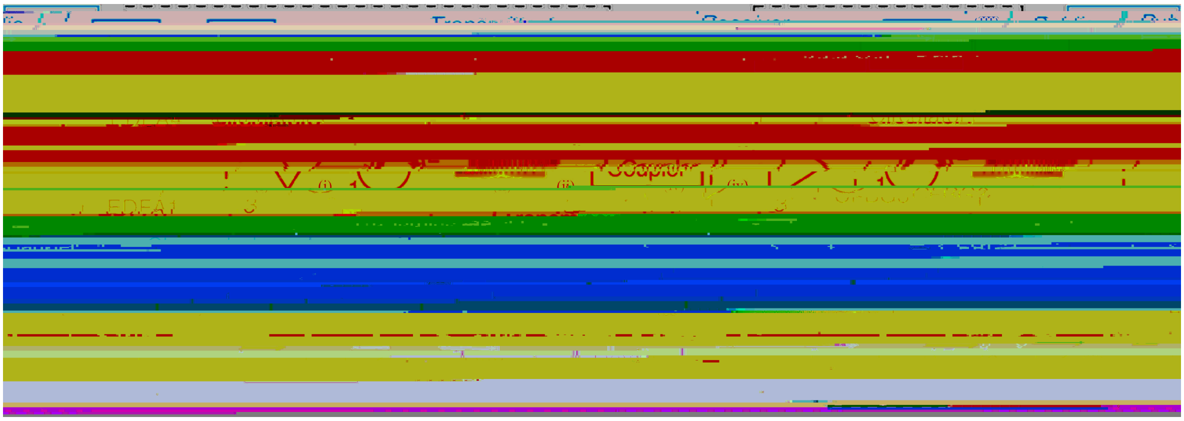
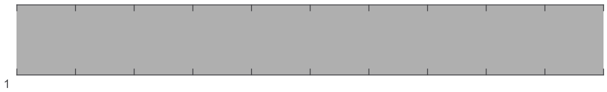


Fig. 2. E e i e al e f he ega g a hic c ica i e . Label (i)-(i), (I)-(VI) c e d h e i Fig. 3 a d Fig. 4.




Windows

he e he ba d id h f blic a d eal h cha el d eed e la .

V. SECURITY ANALYSIS OF SYSTEM PARAMETERS

C e i al ega g a h del e ec he de

A. Hypothesis Testing Problem

H he i e i gi a a i ical e ha i ed de e i e

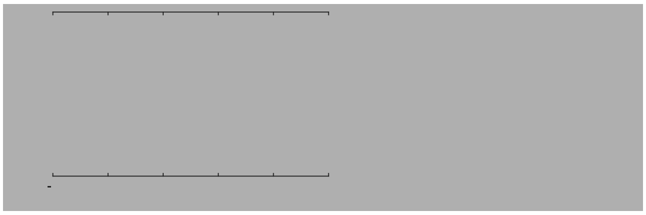


TABLE II
STEALTH SIGNAL CLASSIFICATIONS

where R is the responsivity of the PD, R_L is the load resistance of the PD, $P_{optical}$ is the optical signal power, $P_{electric}$ is the electric signal power, and $I_{electric}$ is the electric signal intensity. When it comes to receiving the data-carrying ASE noise, the electric signal will behave in such a way that

$$I_{electric} = 2RS_{sp}\Delta\nu = C\Delta\nu \tag{10}$$

where S_{sp} is the spectral density of the ASE noise, and $\Delta\nu$ is the ASE noise bandwidth. Meanwhile, several types of electronic noise will be introduced, among which the following three dominate [57], [58]:

$$\sigma^2_{thermal} = 4k_B T F_n \Delta f / R_L = E, \tag{11}$$

$$\sigma^2_{beating} = 4R^2 S^2_{sp} \Delta f \Delta\nu = F\Delta\nu, \tag{12}$$

$$\sigma^2_{shot} = 4qRS_{sp}\Delta f \Delta\nu = G\Delta\nu = H I_{electric}, \tag{13}$$

where k_B is Boltzmann constant, T is the room temperature, F_n is amplification ratio of the electric amplifier in PD, Δf is the electric bandwidth of the PD, and q is the electron charge. The thermal noise $\sigma^2_{thermal}$ accounts for the random thermal activities within a PD, the beating noise $\sigma^2_{beating}$ originates from the interference of various signals at slightly different frequencies within the ASE noise bandwidth, and the shot noise σ^2_{shot} results from the random generation of electrons within a PD whose strength is proportional to the electric signal intensity $I_{electric}$. These three types of electronic noise generated at the PD ought not to be confused with the optical ASE noise even in its origin [illegible] cables.

APPENDIX B
DISPERSION EFFECT/CHIRPED FIBER BRAGG GRATING

The signal transmitted in optical communications typically consists of multiple frequency components (within the signal bandwidth). In an optical media, the transmission speed of each frequency component is inherently different from each other and leads to a temporal spreading of the signal after transmitting over a certain distance. This phenomenon is called dispersion effect, which can be characterized by the dispersion parameter D (in the unit of ps/nm/km). From the perspective of a reliable signal transmission, the dispersion effect should be minimized and needs to be compensated before data demodulation. However, the dispersion effect can also be used to obscure the intensity of modulated signal by lowering the signal power level close to or even below the noise floor, which serves as an enabler for the steganographic communication.

Instead of using the natural dispersion effect resulting from transmitting signal over a long-distance fiber, we intentionally introduce a stronger dispersion effect to the data-carrying ASE noise by using a device called chirped fiber Bragg grating (CFBG) [59]. The CFBG inputs the optical signal from one side, reflects back the signal over a selected bandwidth (called the CFBG bandwidth), and outputs the signal not within the selected bandwidth to the other side. Such a bandwidth selection function is useful for spreading the selected signal because the CFBG reflects different frequency components within its bandwidth at different times, which is equivalent to introducing a huge amount of time delay among frequency components. Being only 20 cm in length, the CFBG can achieve the same dispersion effect as an optical fiber hundreds of kilometers long [60]. Placing two CFBGs with the same bandwidth and dispersion parameters in the opposite orientation makes a perfect pair for signal stretch and compress.

Mathematically speaking, the dispersion effect is illustrated in the signal temporally spread by a *broadening factor* (BF) [61]:

$$BF = \sqrt{1 + \left(2D\Delta\lambda/\tau\right)^2} \tag{14}$$

where D (in the unit of ps/nm) is the dispersion parameter of CFBG, $\Delta\lambda$ (in the unit of nm) is the ASE noise bandwidth used to carry the stealth data, and τ (in the unit of ps) is half of $1/e$-intensity bit width before signal spreading. While all these three parameters contribute to the dispersion effect, we tend to keep $\Delta\lambda$ a small part of the overall transmission channel ASE noise bandwidth in this work, and τ is subject to the electrical I/O speed for users' network interface card.

Note that the total signal energy remains the same even after being temporally spread. Hence, we have the product

$$P_{electric} \times (BF \cdot \tau) = \text{const.} \tag{15}$$

Combining Eq. (9), (14), (15), we have

$$I_{spread} = I_{initial} / \sqrt{BF} \tag{16}$$

that relates the electric signal intensity after signal spreading I_{spread} to that before signal spreading $I_{initial}$ as a function of BF.

APPENDIX C
STEALTH SIGNAL RECOVERY EFFECTIVENESS

SNR_{target} is the stealth signal SNR achieved by the legitimate receiver in recovering the stealth signal after successfully matching $\Delta\nu_{CFBG}$ and D_{CFBG}. The signal and noise terms can both be written following Eq. (9), (10), (11), (12), (13) with the only modification that $\Delta\nu$ is replaced with $\Delta\nu_{CFBG}$:

$$SNR_{target} = \frac{BC^2\Delta\nu^2_{CFBG}}{E + (F+G)\Delta\nu_{CFBG}}. \tag{17}$$

$SNR_{recovered}$ is the recovered signal SNR achieved by the eavesdropper, i.e., $\Delta\nu_{CFBG}$ and D_{CFBG} are to be matched by $\Delta\nu_{eav}$ and D_{eav}. The noise term can be directly derived as

$$P_{noise} = E + (F+G)\Delta\nu_{eav} \tag{18}$$

while the signal term requires more thought. First, PD, Putting together Eqs. (18), (19), we have

$$SNR_{recovered} = \frac{BC^2 \Delta\nu_{Overlap}^2}{E + (F+G)\Delta\nu_{eav}}. \tag{21}$$

We also need to consider matching D_{CFBG} with D_{eav}. Based on Eqs. (10) and (16), we introduce *dispersion recovery ratio (DRR)* that correspond to one of the following *under-compensating*, *over-compensating*, and *extra-spreading* cases:

$$DRR = \frac{\sqrt{1 + \left(D_{eav}\Delta\lambda_{Overlap}/\tau\right)^2}}{\sqrt{1 + \left(D_{CFBG}\Delta\lambda_{CFBG}/\tau\right)^2}} \tag{22}$$

When $D_{eav} < D$

Gaussian process is such that for any choice of distinct values of $t_1, \ldots, t_n \in T$ where T is the observation period, the corresponding signal observations of $\boldsymbol{I} = (I_{t1}, \ldots, I_{tn})$ has a multivariate Gaussian distribution with mean vector $\boldsymbol{\mu}$ and covariance matrix $\boldsymbol{\Sigma}$:

$$p(\boldsymbol{I}) = \frac{1}{(2\pi)^{n/2} det(\boldsymbol{\Sigma})^{1/2}} \exp\left(-\frac{1}{2}(\boldsymbol{I}-\boldsymbol{\mu})^T \boldsymbol{\Sigma}^{-1}(\boldsymbol{I}-\boldsymbol{\mu})\right). \tag{37}$$

Different sequences for bit 0 and 1 observed will lead to different mean vectors $\boldsymbol{\mu}$ and covariance matrices $\boldsymbol{\Sigma}$. Ideally, the bit 0 of the stealth data carries no power, which is equivalent to the case where there is no stealth data for modulation. Hence, the bit 0 carried by the ASE noise is identical to the pure ASE noise at the same bandwidth. Consider the best case for the eavesdropper: the sequence of all 0 (equivalent to no transmitting stealth data) and a sequence of all 1 are observed, which is supposed to result in the largest stealth signal distinguishability. We denote p_{q0}^n for the multivariate probability distribution of the transmission channel signal containing a sequence of all spread 0s, and p_{q1}^n for the multivariate probability distribution of the transmission channel signal containing a sequence of all spread 1s. Their corresponding mean vectors and covariance matrices are $\boldsymbol{\mu}_0^n, \boldsymbol{\Sigma}_0^n$ and $\boldsymbol{\mu}_1^n, \boldsymbol{\Sigma}_1^n$, respectively. Assuming independently measured observations of the transmission channel signal, covariance matrices $\boldsymbol{\Sigma}_0^n$ and $\boldsymbol{\Sigma}_1^n$ are diagonal.

We adopt the same definition in [47], and define that the steganographic communication system is said to be ϵ-*secure on average* if there exists some small ϵ satisfying

$$\lim_{n} \frac{1}{n}$$

[23] J. J a d , "I2 a e k: Technical introduction," Dec. 13, 2010. [Online]. Available: h ://ge i2 . e /e /d c /h /tech-i

[24] L. Boney, A. H. Tewfik, and K. N. Hamdy, "Digital watermarks for audio signals," in *Proc. 3rd IEEE Int. Conf. Multimedia Comput. Syst.*, Jun. 1996, pp. 473–480.

[25] C.-T. Hsu and J.-L. Wu, "Hidden digital watermarks in images," *IEEE Trans. Image Process.*, vol. 8, no. 1, pp. 58–68, Jan. 1999.

[26] R. G. van Schyndel, A. Z. Tirkel, and C. F. Osborne, "A digital watermark," in *Proc. IEEE Int. Conf. Image Process.*, Nov. 1994, vol. 2, pp. 86–90.

[27] R. B. Wolfgang and E. J. Delp, "A watermark for digital images," in *Proc. Int. Conf. Image Process.*, Sep. 1996, vol. 3, pp. 219–222.

[28] R. J. Anderson and F. A. Petitcolas, "On the limits of steganography," *IEEE J. Sel. Areas Commun.*

Alexander N. Tait received the Ph.D. degree from Professor Paul Prucnal in the Lightwave Communications Research Laboratory Group, Department of Electrical Engineering, Princeton University, Princeton, NJ, USA. He is an NRC