ABSTRACT
Security in communications is an important issue in rapidly growing information-oriented society. We are proposing a novel method of secure communications using chaotic semiconductor lasers. Here, we discuss encryption of messages into irregular signals produced by chaotic semiconductor lasers and decryption of them based on chaos synchronization between nonlinear transmitter and receiver systems.

1. INTRODUCTION
It was forty years ago that Lorenz, investigating the behavior of convective fluid flow as a model for the atmospheric flow, showed that nonlinear systems described by three variables could exhibit chaotic dynamics.[1-3] Chaos is the phenomenon of irregular variations of system output derived from models described by deterministic equations. In spite of the deterministic models, we cannot foresee the future of the output since chaos is very sensitive to the initial conditions and each system behaves completely different from each other even if the difference of the initial state is very small. Chaos can be observed in various fields of engineering, physics, chemistry, economics, and biology. Though the fields are different, some of the chaotic systems can be characterized by similar differential equations.

Since lasers are nonlinear systems and are typically characterized by three variables; the field, the polarization of matter, and the population inversion, they are candidates for chaotic systems. Indeed, it was proved in the mid 70’s by Haken [1-2] that lasers are nonlinear systems similar to the Lorenz model and they show chaotic behaviors in the sense of performance or ease of implementation. Therefore, the laser rate equations that are described by the nonlinear equations with three variables and involve chaotic dynamics are called Lorenz-Haken equations after their contribution [1-2]. However, ordinary lasers do not exhibit chaotic behaviors and only a few of the lasers with bad cavity conditions show chaotic dynamics. In the meantime, chaotic behaviors were theoretically demonstrated in a ring laser system [1-2]. In the meantime, important breakthroughs for the applications of chaos have been done in the early 90’s.[1-3] The ideas of chaos control and chaos synchronization have been proposed and developed for the decade. The idea of chaos control has been immediately applied to the stabilization of chaotic lasers. The possibility of chaos communications has been discussed based on chaos synchronization in two chaotic laser systems.[3]

In this paper, we focus on the method of secure optical communications in chaotic semiconductor lasers induced by optical feedback. Since fast chaotic oscillations on the order of GHz fluctuations are easily produced by the system, optical feedback induced chaos in semiconductor lasers is frequently used as a generator for chaotic communications. The key technology for chaotic communications is chaos synchronization in the system. At first, we discuss the general idea of chaotic communications in nonlinear systems and the method of chaos synchronization in laser systems. Then, we describe chaos synchronization and chaotic communications in semiconductor lasers with optical feedback. We acknowledge that the particular schemes described in most detail here may not be the best suited for practical applications in the sense of performance or ease.
of implementation. However, they effectively demonstrate key aspects of the physics of recovering messages by chaos synchronization in lasers.

2. CHAOTIC SECURE COMMUNICATIONS

Chaos is generated in a system described by a set of deterministic equations and gives rise to irregular fluctuations similar to random signals. However, it is completely different from phenomena of events in stochastic process. In chaotic oscillations, we cannot foresee the future of the evolution of the system, since chaos is sensitive to the initial conditions of the system and they are always different for each trial in actual systems.[2,4] Therefore, we cannot expect the same or similar output for any two nonlinear systems as far as they are isolated, even if they consist of the same components and have the same parameters.

On the other hand, under appropriate parameter conditions, the two systems can synchronize with each other when a small fraction of one of the system is transmitted to the other. The scheme is called chaos synchronization.[3] The key technology for chaotic secure communications is chaos synchronization. In chaotic communications, we must use transmitter and receiver systems with the same characteristics including the values of the parameters. Even when the transmitter and receiver are the same systems, chaos synchronization is not achieved as far as the parameter values of the two systems are different. This guarantees the security of the communication between the two systems. Namely, the parameter values are the keys for secure communications.

Progress in the understanding of mechanisms and techniques for the controlled generation of chaos in lasers has lead to efforts to apply laser chaos in communication systems. Random and pseudo-random signals are widely used in modern communication systems to encode data for the purpose of reducing errors in detection or to ensure that data is only received by the intended receiver. In recent years, work has begun on developing chaotic algorithms, algorithms using the iteration of nonlinear functions, to efficiently generate random sequences with improved randomness and correlation properties for use in spread-spectrum, code-division multiplexing and error correction [5]. Also, research on the physical generation of chaos in electrical circuits and optical devices has lead to various investigations of the use of chaotic waveforms as physical signal carriers. Some of the earliest ideas on chaotic signal carriers involved the use of chaotic waveforms as easily generated, wideband carriers for spread-spectrum modulation schemes. Subsequent work sought to exploit synchronization properties of chaos, mostly focusing on the idea of secure communication applications.

In recent years, a good example of an implementation of a communication scheme based on synchronized chaos is the demonstration by Tang and Liu using semiconductor lasers with opto-electronic feedback to transmit low error non-return-to-zero (NRZ) signals at the bit rate of 2.5Gbps which corresponds to the data rate of the widely used OC-48 standard for optical connections [6,7]. The degree of the security in optical communications is strongly dependent on the contents to be communicated. The studies for the degree of the security and robustness in chaotic communication systems and are still under way and a lot have still been left for the future issues. This report is the current state-of-the-art results of optical secure communications in chaotic semiconductor lasers with optical feedback done by our research.

3. LASER CHAOS SYNCRONIZATION AND CHAOTIC COMMUNICATIONS

In this section, we discuss chaos synchronization in laser systems and analogue chaotic communications based on chaos synchronization. Figure 1 shows a schematic illustration for a system of chaotic secure communication.[3] In a
chaotic transmitter, a signal with irregular chaotic oscillation is generated and a small portion of the output is sent to a receiver. The receiver consists of the same system of the transmitter or the subsystem of the transmitter. Therefore, the receiver system itself may be a chaotic or stable system without the transmission of a signal from the transmitter. Upon receiving a transmitter signal, the receiver reproduces the same chaotic signal as the transmitter under appropriate conditions of the system parameters. It is noted that the same parameter values between the transmitter and receiver do not always guarantee successful chaos synchronization.

In chaos synchronization, there are two schemes of synchronization. One is complete chaos synchronization and the other is so called generalized chaos synchronization. In complete chaos synchronization, the receiver system is described by the equivalent differential equations as those of the transmitter and the receiver laser transmitter. Therefore, good synchronization is expected in a complete chaos synchronization scheme. On the other hand, synchronization is achieved by the amplified injection locking in a generalized chaos synchronization. In this case, the chaos parameters may not be equal with each other in the transmitter and receiver systems and the two systems may have small parameter mismatches.

In either case of synchronization schemes, chaotic communication is similarly performed. A small message is embedded into the chaotic carrier in the transmitter and they are sent to the receiver. In the receiver system, only chaotic signal is reproduced. This is known as a chaos-pass-filtering effect in nonlinear systems. Therefore, the message is extracted from the subtraction of the receiver output from the transmitted signal. The theoretical background of chaos synchronization and chaos-pass-filtering effects have not been well established. However, they are confirmed by numerical simulations and experiments.

As chaotic generators, chaotic lasers are frequently used, since laser chaos is best suited for optical communications. Solid-state laser, fiber laser, and semiconductor laser have been used as light sources for chaotic laser generators. Among them, semiconductor laser is the best candidate as a chaotic laser generator, since it is a compact device and it can generate fast chaotic carrier signal. Semiconductor laser itself is a stable laser called class B-laser in its solitary oscillation. However, it is easily destabilized by external perturbations; for example, optical injection, injection current modulation, and external optical feedback. In the following section, we focus on chaos synchronization and chaotic communications in semiconductor lasers subjected to optical feedback.

4. CHAOS SYNCHRONIZATION IN SEMICONDUCTOR LASERS WITH OPTICAL FEEDBACK

Semiconductor laser destabilized by optical feedback and shows chaotic behaviors. The instability is reproduced by the use of the laser rate equations including external optical feedback.

![Fig. 1 Schematic diagram of chaotic communications.](image)

![Fig. 2 Chaos synchronization systems using semiconductor lasers with optical feedback](image)
Though the instability depends on the laser device structures and optical feedback level, chaotic behaviors are observed even for a small fraction of optical feedback as less than $10^{-4}$% optical feedback in intensity. The noise level is also compatible with optical feedback in compact disk (CD) systems and the noise induced by optical feedback in those is not a simple noise but a chaotic fluctuation. Noise reduction has been also proposed based on chaos control technique. The dynamic properties of chaotic semiconductor lasers are important issues not only for basic research in nonlinear systems but also for various applications. Here, we introduce chaos synchronization in semiconductor lasers with optical feedback.

Figure 2 shows different chaos synchronization schemes in optical feedback induced chaotic semiconductor lasers. Fig. 2(a) is an open-loop chaos synchronization system. The transmitter is a chaotic system of a semiconductor laser with optical feedback, while the receiver is a solitary laser. In a certain operation condition of the laser, the transmitter laser shows a chaotic oscillation and a small portion of chaotic signal is sent to the receiver laser. Under appropriate set of the parameter values of the transmitter and receiver lasers, the receiver laser exhibits the same or similar output as the transmitter laser. Fig. 2(b) is a symmetrical system called closed-loop chaos synchronization system. The receiver system may either output chaotic oscillation or stable oscillation without transmitting the transmitter signal. Even when the receiver laser exhibits a chaotic oscillation, it never shows the same or similar waveform as the transmitter laser because of the sensitivity of the initial condition of chaotic oscillations. However, in the presence of the signal transmission, the receiver laser synchronizes with the transmitter signal under appropriate conditions of the parameter values. In actual, the system in Fig. 2(a) is the special case of Fig. 2(b). When we put the reflectivity of the external mirror in the receiver system zero, then the system in Fig. 2(b) becomes equal to the system in Fig. 2(a). Though the performance of chaos synchronization and the degree of the security for chaotic communications are different with each other in those two systems, we can study the dynamics of chaotic behaviors and the performance of chaos synchronization by using the same rate equations.

![Image](image)

Fig.3 Example of chaos synchronization

Figure 3 shows an experimental example of chaos synchronization in the closed-loop system shown in Fig. 2(b). Two lasers with quite similar characteristics are selected from lasers of the same product number and they are operated at almost the same conditions. The two lasers exhibit completely different outputs without the transmission of signal from the transmitter to the receiver. But, by an optical injection from the transmitter to the receiver lasers, the receiver laser shows the same output as that of the transmitter laser as shown in Fig. 3. The synchronization shown in Fig. 3 corresponds to the scheme of generalized chaos synchronization. When the device parameters are given in advance, the conditions for successful chaos synchronization are determined by numerical calculations based on the laser rate equations.[8]

5. CHAOTIC COMMUNICATIONS IN SEMICONDUCTOR LASERS WITH OPTICAL FEEDBACK

Methods for transmitting messages using optical-feedback induced chaos can be divided into three categories depending on the scheme for
They are chaos shift keying (CSK), chaos masking (CMA) and chaos modulation (CMO). Figure 4 shows examples of schematic circuit diagrams for each category. In each case, there is a semiconductor laser with feedback to generate chaos on the transmitter side and on the receiver side. Messages are imposed on the chaotic carrier signal generated in the laser by modulating the laser injection current or modulating the laser light signal itself. At the receiver end, a similar laser is prepared so that it will synchronize to the corresponding chaotic state when the light transmitted from the transmitter laser is injected into it. Message recovery is performed by detecting the difference between the injection signal and the receiver laser output signal.

In the method known as chaos shift keying (CSK) the injection current of the transmitter laser is modulated with a bit sequence to switch the transmitter laser output between two different chaotic states corresponding to “1” and “0” bits. If the receiver laser can only synchronize to one of these states, the switch can be detected by comparing the signal output from the receiver laser with the injected signal and testing for synchronicity. A disadvantage of this method is that the bit rate is limited by the synchronization acquisition time and accordingly it is difficult to achieve high bit rates.

Before showing chaotic secure communication, we demonstrate the effect of chaos-pass-filtering in a system of a semiconductor laser with optical feedback. Figure 5 shows the spectra for the chaotic transmission signal including a message and the synchronized receiver output. The message is a sinusoidal signal of a frequency of 1.5 GHz. We can see chaotic transmission signal of the transmitter laser output together with the message spectrum at 1.5 GHz. However, we cannot see clear spectrum of 1.5 GHz in the receiver output. This is the effect of chaos-pass-filtering. It may seem that the message can be extracted from the transmission signal as shown in Fig. 5(b). However, the phase information is fairly disturbed by the chaotic signal and the complete information of the original signal cannot be reconstructed from the analysis of the transmitted signal. This guarantees the security of the data transmission based on the effect of chaos-pass-filtering.

Figure 6 shows the numerical results of chaos communications based on the ON/OFF chaos shift keying (CSK).[9] The message is a pseudo-random-bit sequence of 2 Gbps. Figs. 6(a)
and (b) are chaotic transmission signals without and with a message. Fig. 6(c) is the receiver output. Fig. 6(d) is the recovered message after a low-pass filtering. The original bits are successfully reconstructed.

6. CONCLUSION

We have demonstrated the method of secure communication based on chaos synchronization in systems of chaotic semiconductor lasers. Since laser chaos is best suited for existing optical communication systems, the proposed technique is useful in practical applications. The feasibility study for chaotic secure communications has just been started and much have been left for the future issues.[10,11]

REFERENCES