Technical journals online.com

Research Article

DETAILED SCHEMATIC TO IMPLEMENT: A HIGH-SPEED CHAOTIC OPTICAL COMMUNICATION SYSTEM WITH DYNAMIC KEY

Saha Panthadeb[*a], Sarkar Anindita [b]

Address for Correspondence

[a]B. P. Poddar Institute of Management & Technology, 137 VIP Road, Kolkata-700052, WB
[b]Netaji Subhash Engineering College, Panchpota, Garia, Kolkata-700152, WB India

ABSTRACT:
Here we have shown the schematic in detail for implementing a high speed chaotic optical communication system with the external optical feedback path length as its dynamic key for digital data transmission. This dynamic key is message dependent and hence time varying also. This makes the system more secure and reliable compared to other existing encryption systems.

KEYWORDS: chaos; dynamic key; external cavity semiconductor laser; optical communication.

1. INTRODUCTION

To achieve security and reliability in high-speed secure communication technology chaos is applied over optical data transmission, and cryptographic systems are implemented. With advancement of technology the key to data encryption in optical domain requires to be dynamic i.e. varying. The need of a dynamic key in secure optical communication is justified in [1]. In [2] we have proposed such a optical cryptographic system where we set the external optical feedback path length of a long-external cavity laser (ECL) operating in a chaotic state as a message dependent key for chaotic optical communication, which makes it varying with message and hence with time and establishes it as a dynamic key.

2. THE PROPOSED SYSTEM AND THE DYNAMIC KEY

A. Schematic in Basic Building Blocks

The schematic of the proposed system is shown in basic building blocks as fig. (i) for the optical chaotic encryption system and as fig.(ii) for the decryption system.

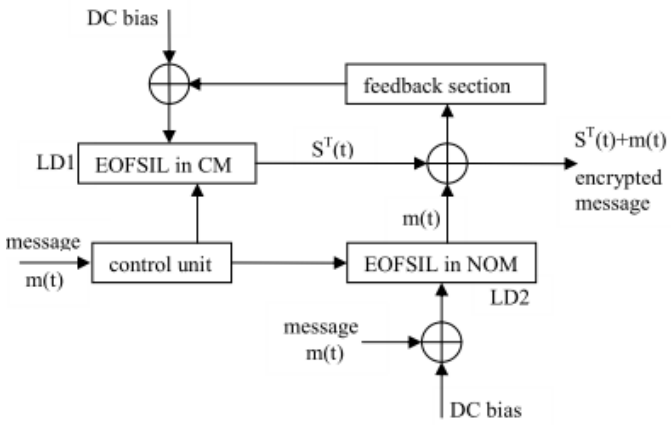

Fig. (i). basic building blocks of the optical chaotic encryption system.

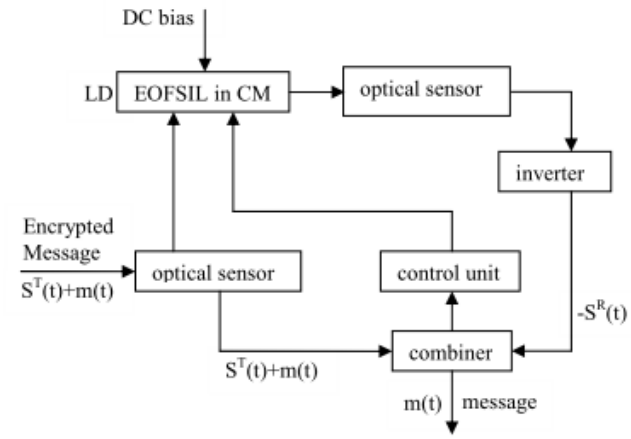

Fig. (ii). basic building blocks of the optical chaotic decryption system.

B. System Description

Transmitter end (encryption system)

Here we choose the laser diodes which are single mode with multistability. The laser diode LD1, is an external optical feedback semiconductor injection laser (EOFSIL) diode operating in chaotic mode (CM) by the proper choice of system parameter values e.g., driving current, optical path length, external optical feedback amount. The other parameters except the optical path length inside the diode external cavity are kept constant throughout a single transmission. We set the external cavity length of the laser diode i.e. the optical feedback path length as the key to the cryptographic system. Here the optical path length inside the external cavity is changed from time to time during a single transmission so that the wavelength of the emitted light changes correspondingly. The external cavity lengths are selected from the raw message bits based on a definite logic. This makes the key of the system

message dependent and hence time varying also. There is another laser diode LD2, which is also a external optical feedback semiconductor injection laser diode operating in normal operating mode (NOM) and emitting message in the form of optical signal. This is then mixed with the chaotic output by the simple method of addition of amplitudes and sends to the receiver. A portion of the finally emitted signal is feedback to the laser diode in chaotic mode through an electro optical feedback network to keep it in a steady state. The two laser diodes are made wavelength matched by a control unit. The raw message bits are send serially to the laser diode emitting message in the form of optical signal i.e., in every unit of time a certain amount of message bits in the form of electrical signal are passed through a message queue. The control unit takes few numbers of bits from certain predefined positions of the message queue in a unit of time and generates a voltage following a predetermined logic. This voltage is then applied to the electrically tunable Fabry-Perot Interferometer (FPI) filters placed inside the external cavity of both the laser diodes simultaneously so that they can emit an identical wavelength at the same unit of time, hence they are made wavelength matched. The electrically tunable FPI filters contain nano-sized nematic liquid crystal droplets as their active material. They support only one of their resonance wavelengths at a time depending on the magnitude of voltage applied across it. Because depending on the magnitude of voltage the nano-sized nematic liquid crystal droplets orient themselves at a particular angle which results a particular refractive index of the active material and hence they support a particular wavelength (called resonance wavelength) at a time.

The optical path length inside the external cavity is varied by varying the refractive index of the liquid crystal material (liquid crystal droplets) of the electrically tunable FPI filter, by applying suitable voltage across it. But the response time of such liquid crystal materials are much longer compared to optical data transmission speed. Due to this reason when the refractive index of a liquid crystal material changes by changing the magnitude of applied voltage i.e. the interval of time which should elapse before the liquid crystal droplets settles to a new orientation to give a new refractive index on application of the required magnitude of voltage, some encrypted message will be transmitted with some uncertain values of the refractive index which may cause severe error during decryption at the receiver end. So a double external cavity is used for alternate transmission, where, when one cavity is active, during that time the other one is made ready for transmission. The second cavity in this time is kept optically isolated from the system by using optical isolator or polarizer. The polarizer should response at minimum response time. Here external cavities are used alternatively in every alternate unit of time. Though in every unit time block any one of the external cavities is active and determines the optical path length in it and hence the frequency of transmission but at the junction of two unit time blocks(which is a little fraction of a unit time) when changeover between the two cavities takes place both of them remains active and so the encrypted message is carried by two frequencies during that time because it requires a little fraction of time to completely optically incorporate and optically isolate a cavity from the system. This will not create any difficulty at the receiver end to faithfully decrypt the message or not help intruders any way to extract the information from the transmitted message. Here in the ongoing unit time block the frequency corresponding to this cavity will be considered as the primary frequency and in the next unit time block the frequency corresponding to the other cavity will be considered as the primary frequency. Only during this transition time at the junction of two unit time blocks the laser acts as a dual cavity laser which has a benefit. According to [3] if radiation is constantly injected into one or more modes of a modulated laser it is quite effective as a means for suppressing the relaxation oscillation and reducing the response delay in the modulated output of a semiconductor laser.

Receiver End (decryption system)

To recover the message, a replica of the chaotic carrier is reproduced at the receiver end, which is achieved through chaos synchronization. According to the theory of chaos synchronization two identical systems, the transmitter and the receiver systems are synchronized in chaotic states by perfect parameter matching and are driven by a common force. Message decoding is then achieved by removing the chaotic carrier from the received signal at the receiver. On the other hand, eavesdroppers cannot recover the message because of the lack of information about the parameters and also due to their nature of variation with time.

Since the two lasers LD1 & LD, are made parameter matched, they can synchronize and the receiver laser will reproduce the chaotic carrier output of the transmitter laser. The message is recovered by subtracting the reproduced chaotic waveform at the output of the receiver laser from the received signal through an inverter and a combiner.

At the transmitter end the message m(t) is encoded by additive chaos modulation as $S^T(t) + m(t)$ after the light comes out of the transmitter laser, with $S^T(t)$ the chaotic output of the transmitter laser LD1. On the receiver end, the receiver LD laser is driven by $S^T(t) + m(t)$, which is the same force that drives the transmitter. When the two lasers are parameter matched, they can synchronies and the receiver laser can reproduce the chaotic output of the transmitter laser as $S^R(t) = S^T(t)$. The message is recovered by subtracting the reproduced chaotic waveform at the output of the receiver laser from the received signal through the inverter and a combiner as $S^T(t) + m(t) - S^R(t) = m(t)$.

The two initial voltages V1 & V2 should be known at the receiver end as the key to the encryption system and are readily applied to the FPI filters FPI1 & FPI2 respectively of the laser diode LD.

3. THE SCHEMATIC IN DETAIL

The operation of the system is explained with a illustration in [2].

These basic building blocks can be implemented as shown elaborately in fig.(iii) for the transmitter end and fig.(iv) for the receiver end. In fig. (iii) and (iv) the solid lines with arrows gives the direction of flow of electrical signal and dotted lines with arrows shows the direction of flow of light. The dashed lines indicate the optical path lengths where L_D is the laser cavity length and L_{ext} is the external optical feedback path length.

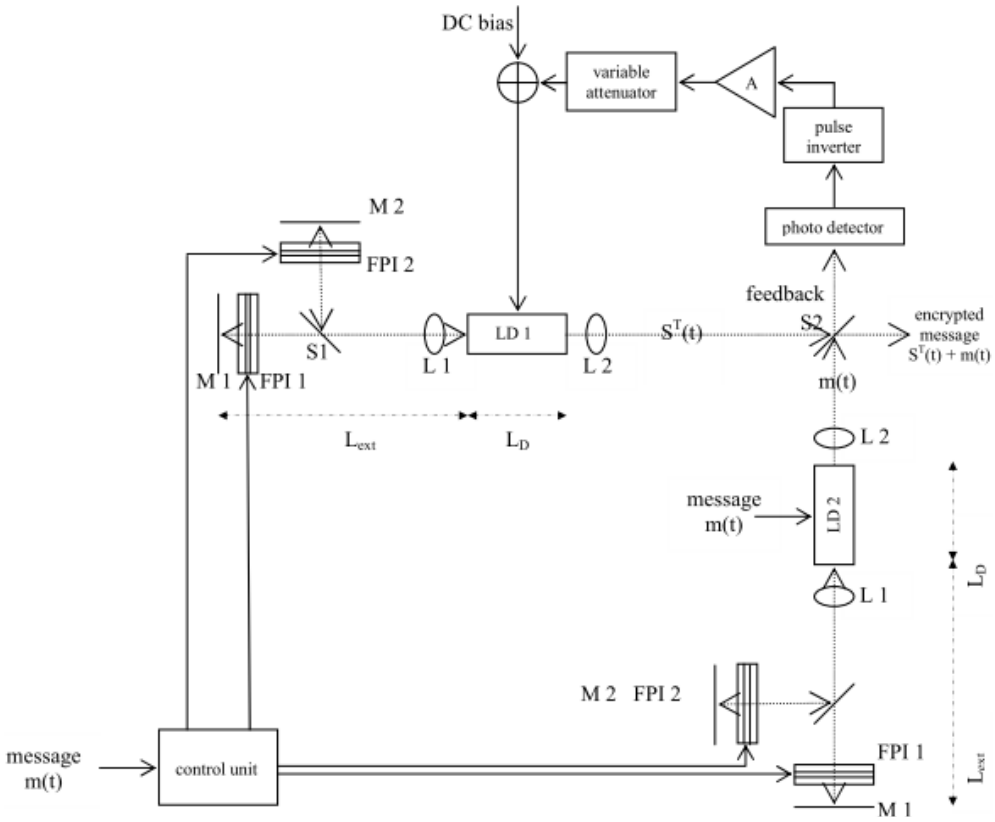

fig.(iii). Implementation scheme for the optical chaotic encryption system

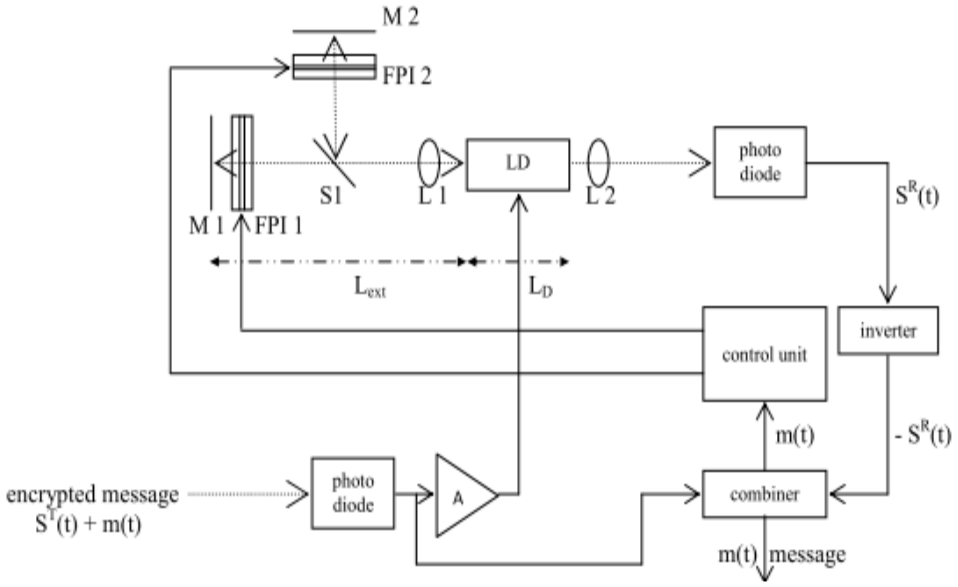

fig. (iv). implementation scheme for the optical chaotic decryption system

The control unit includes the message queue and will apply the proper voltages to the FPI filters accordingly. The beam splitter-cum-combiner S1 is placed in the external feedback path to make use of dual external cavity. The beam splitter S2 is used to provide signal to the laser diode LD1 which is in chaotic mode through a electro optical feedback network to keep it in a steady state. M1 and M2 are indicated as mirrors to imply returning of light back to the respective semiconductor lasers. L1 and L2 are lenses used in conjunction with the lasers as usual.

Tuning Range

The Electrically tunable FPI filters have a cavity layer sandwiched between mirrors and transparent electrodes. Light satisfying the resonance condition is transmitted through the filter. This condition is given by, $\lambda_m = 2\eta L/m$ where, λ_m is the wavelength of the transmitted light, η is the refractive index of the cavity material, L is the cavity gap, and m is an integer. When the refractive index is changed by applying a voltage, the transmitted wavelength (resonance wavelength) shifts so that this equation is satisfied. The resonance wavelength shifts gradually with increasing voltage. The tunable range is $2\Delta\eta L/m$ [4].

As reported in [5], when the voltage applied to the FPI filter is increased, the peak wavelength is decreased. The wavelength decrease approaches saturation at around 450V. The wavelength shift was about 5 nm at 200V, 10 nm at 300V and about 13 nm at 450V in the 1.55 μ m wavelength range. These shifts are smaller than those with FPI filters using bulk nematic liquid crystal but it is polarization independent and has faster switching (370 μ s) and there is no threshold voltage also. The change in refractive index $\Delta\eta$ of a polymer containing nano-

sized nematic liquid crystal is proportional to the square of the applied field E, i.e., $\Delta\eta = kE^2$, where k is the proportionality constant was taken to be equals to $5\times10^{-5}(\mu m)^2/V^2$.

However the length of the unit time frame will ultimately be governed by the response time of the FPI filters i.e. by the switching speed of the nano-sized nematic liquid crystal and the response of the other electrical counter parts. But it is obvious that the system will be more and more secured as the length of the unit time frame will be decreased.

4. DISCUSSION

As technology advances security measures enhances in the field of communication technology also. But it is seen that those security measures are breeched with time by a third party. This is also a reason of advancement in technology. But if the security measures are made dynamic i.e., varying then it becomes absolutely impossible for a third party to breech it. Here in the developed model the dynamicity is not only in time but also spatial. Thus it provides security to a higher degree compared to such other existing systems.

REFERENCES

1. Qingchun Zhao, Yuncai Wang, and Anbang Wang, "Eavesdropping in chaotic optical communication using the feedback length of an external-cavity laser as a key", Applied Optics, vol. 48, issue 18, pp. 3515-3520 (2009).
2. Saha P, Sarkar A, " A Dynamic Key for High-Speed Chaotic Optical Communication" IJAERS , Vol. 2 , issue 2 , pp. 40-45.
3. Roy Lang & Kohroh Kobayashi, "Supression of the Relaxation Oscillation in the Modulated Output of Semiconductor Laser", IEEE J.Q. Electronics, vol. QE-12, NO. 3, March 1976, pp.194-199.
4. K.Hirabayashi, H.Tsuda & T.Kurokawa, "Tunable Liquid- Crystal Fabry-Perot Interferometer Filter for Wavelength-Division Multiplexing Communication Systems", J.Lightwave Tech., vol. 11, NO. 12, Dec. 1993, pp.2033-43.
5. S.Matsumoto, K.Hirabayashi, S.Sakata & T.Hayashi, "Tunable Wavelength Filter Using Nano-Sized Droplets of Liquid Crystal", IEEE P. Tech Lett., vol. 11, NO. 4, March 1999, pp.442-4.
6. R.Lang & K.Kobayashi, "External Optical Feedback Effects on Semiconductor Injection Laser Properties" IEEE J.Q. Electronics, vol. QE-16, NO. 3, March 1980, pp.347-55.
7. S.Tang & J.M.Liu, "2.5Gb/s Chaotic Optical Communication", OFC 2002, pp. 402-3.
8. J.Paul, S.Sivaprakasam, P.S.Spencer, P.Rees & K.A.Shore, "GHz bandwidth message transmission using chaotic diode lasers", IEE Elect. Lett. Vol. 38, no. 1, Jan. 2002, pp.28-9.