



Secure optical communication using chaos

R. Raja Kumar, A. Sampath and P. Indumathi¹

Mathematics Department, Sathyabama University, Chennai-600119, India.

¹*Electronics Engineering Department, MIT Campus, Anna University Chennai-600044, India.*

rrkmird@yahoo.com; dr_asampath@yahoo.co.in; indu@mitindia.edu

Abstract

In this paper we demonstrate a way to secure optical communication. Chaos as a tool for information security is gaining wide acceptance for its inherent simplicity and ability to secure a communication link from the physical layer compared to other application layer-software encryption methods. Though they are lesser secured than the physical layer systems, the software techniques are still the order of the day. Since the physical layer techniques are still in the nascent stages of growth, this paper tries to go one step further, to utilise the chaotic scheme in securing optical communication. The idea is to generate a chaotic signal in the form of current and adding it to the message at the transmitter where the whole of this current drives an optical source-laser. At the receiver the same chaos signal is generated by prior synchronization. The received signal is photodetected to get the equivalent current. The difference between this current and the internally generated matched chaos yields the message. The efficiency of this technique is investigated for line of sight communication by modelling a free space optic channel (FSO) and accounting for attenuation caused by the same.

Keywords: Chaos, cryptography, secure optical communication

Introduction

Optical communication is being used widely these days. Though it has inherent advantageous features such as being immune to Electro Magnetic Interference (EMI), and additional safety features like some amount of immunity to tapping, it still fails because a user is not guaranteed complete security of the data. Since the physical layer techniques are still in the nascent stages of growth, there is a need to go one step further, to utilise the chaotic scheme in securing optical communication (Valerio Annovazzi *et al.*, 2008).

This paper tries to explore chaotic communication in a way so as to effectively use it for secure optical communication. Optical communication systems use either LASERS or LEDs as the transmitter. LASER systems are preferred for long distance communication needs. LASER systems are often compared and contrasted to their counterparts-the LEDs. LEDs are cheap, preferred over small distance links and have large spectral width of emission. The LASER systems are costlier, used for long distance optical communication links and have a very narrow spectrum of emission. Since we tried to simulate a method that could secure long distance optical communication like those used in links between satellites, we modeled LASERs. The same method can be implemented using LEDs for short hauls. Here we design the chaotic function based on bifurcation function and as a process of analysing the performance, we model the system i.e., the individual components making up the whole communication system including the laser, FSO channel and the photo detector. The performance is verified.

Chaotic communication

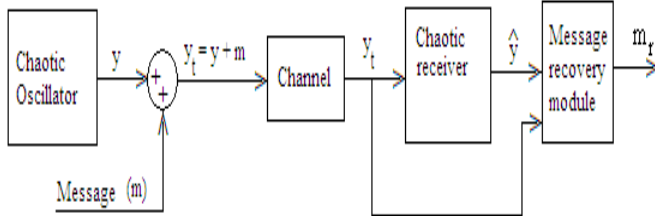
Assume a ball placed on the top of a mountain peak. Even slightest differences in this initial position make the ball roll along any of the slopes of the mountain. We observe that the system properties or dynamic behaviour depends on the initial conditions, and the value of the system at any instant (the position of the ball at any instant in this example) depends on the value of the system at all previous instants. This behaviour is called chaotic behaviour and the system, a chaotic system. Thus we see the system is very sensitive to initial conditions. Also the values of the system are sequentially related but apparently random. Hence it becomes increasingly difficult for the interferer to intervene because even the small mistakes committed in estimating the initial values diverge exponentially leading to unintelligible outputs at a later time.

We can expect chaotic behaviour from any dynamic system that shows sensitivity towards initial conditions. Such systems show a very high relationship with the previous values so that the value of the system at any point of time depends on the previous values.

This makes us conclude that small differences in initial conditions yield widely diverging outcomes for chaotic systems. Hence the outcome varies every moment-in fact diverges exponentially similar to a chain reaction. Also that the value of the event (its magnitude in whichever form is measurable) at this moment depends on all the values experienced in the previous instances of time. And, we can add to that, the most admirable quality that even a small error in marking the initial position shall mean that value marked at any other instant after that moment is completely erroneous.

Cryptography is the method for safeguarding information from eavesdroppers. In other words it is the science of encrypting information for security. A security key is used for encryption here. In symmetric key systems, the same key is used at the receiver's end to

Fig.1. Simple chaotic communication system



decrypt the message. But due to the improved calculating efficiency of modern computers and intellect of hackers these systems are more vulnerable to threat nowadays. But imagine a situation, in which an eavesdropper tries to interpret a signal; we see that he cannot do his job if the secret key varies every moment or if the value of the secret key at this moment depends so much on the secret key used at the beginning, or if the method used for encryption is so sensitive that even an error in the seventh or eighth decimal position made by the hacker leads to a total haywire.

This establishes the fact that chaotic system possesses ideal characters to be employed in crypto systems. By using chaotic methods we can prevent all kinds of intrusions. Fig.1 shows a simple system that uses chaos for security. A very easy way to safeguard the message is to hide it with the chaos and send it. It can be completely retrieved at the receiver's end by generating the same chaos.

Bifurcation and the chaotic function

Chaotic Map

This chaos described can be generated mathematically. Recursive algorithms can be used to calculate the values. That is we see any X_i th value depends immediately on X_{i-1} th value. Hence the value can be recursively calculated. But this way of recursively doing is computationally complex compared to doing by mathematical equations. Hence it is simpler to use mathematical equations as each step involves only two floating point multiplications and a subtraction (refer equation 2).

Consider the following function:

$$f(x) = p * x * (1 - x) \tag{2}$$

this is a second order function that can be used to generate mathematical chaos. We see that this equation is bounded for the limits $0 < p < 4$.

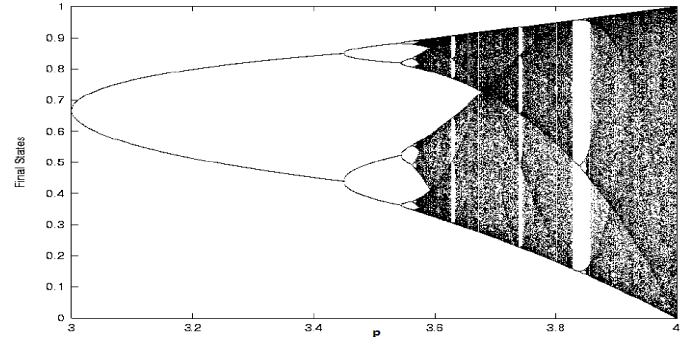
In other form the same equation can be written as

$$x_{n+1} = p * x_n * (1 - x_n) \tag{3}$$

with x_0 as the starting value. This is

the iterative form where we see every nth value depending on all other previous values. The plot of such functions is also called chaotic maps (Larger *et al.*, 2005). The chaotic map of the above function is given below and this answers to why p is bounded as we see for that

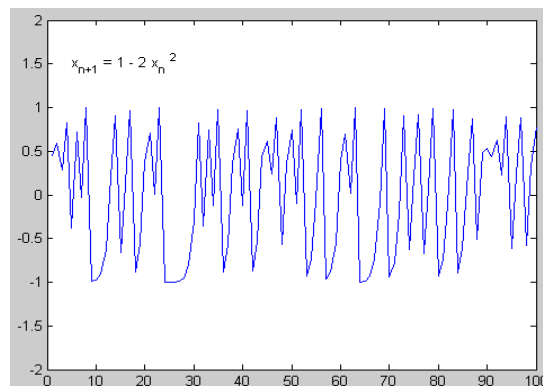
Fig.2. The "bifurcation diagram" for the function $f(x) = p * x * (1 - x)$



bounded value of p, the system loses its periodicity and behaves chaotically.

Fig.2 shows the "bifurcation diagram" of this function. Bifurcation is defined as the process of division into two or more branches. When we plotted the above function (3), with x_0 as the starting value we got the output as in figure 2. This is a plot of the parameter 'p' with the values that are obtained after some number of iterations. For $0 < p < 3$, the function is seen to converge to a particular value after some number of iterations. As p is increased to just greater than 3 the curve splits into 2 branches. This splitting is called bifurcation. Mathematically this leads to chaos. The values generated by this function now oscillate between two different values. As the parameter 'p' is further increased, the curves bifurcate again and now the oscillations are seen in between 4 values. As 'p' is further increased the bifurcations become faster and faster, 8, 16 then 32. Beyond a certain value of 'p' known as the "point of accumulation" periodicity gives way to complete chaos. This is found for $p > 3.57$. The chaos values generated at this point are seen to be restricted to two different bounds. Finally for $p = 4$, we observe that chaos values are generated in the complete range of 0 to 1. It is this point that we are interested in. As mentioned earlier, a slight difference in the initial starting value i.e.

Fig.3. Generated chaos signal

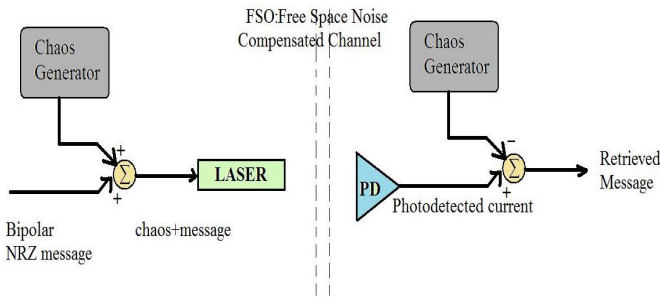


X_0 leads to substantial difference in the obtained iterative values. This Fig. 2 is a plot of the parameter 'p' with the values that are obtained after some number of iterations. We see in the limits bounded by $0 < p < 3$, the function is seen to converge to a particular value. But after $p > 3$ the curve splits leading to a small value of randomness. However during $3.6 < p < 4$, the plot shows complete randomness and

chaotic behaviour.

From the plot of Fig.3 (plot of $x(n)$ Vs n), we see that the values generated by this function now oscillate between two different values 0 and 1 for $3.6 < p < 4$. The values are limited between 0 and 1, but still they are apparently random and totally non periodic. Finally for $p=4$, we observe that chaos values are generated in the complete range of 0 to 1. It is this point that we are interested in. As mentioned earlier, a slight difference in the initial starting value i.e. x_0 leads to substantial difference in the obtained iterative values.

Fig. 4. The communication system model



System model

The system is as shown in Fig.4. It consists of three individual components (Larger *et al.*, 2005), namely, the LASER that acts as the source, the extinction modelled free space and the photo detector. Each of these components can be modelled as follows. We need not use any kinds of modulator or demodulator in this method. We just add the chaos to the message and give the resultant signal to the optical source(LASER) and receive it at the optical destination(photodiode).

Laser model

We need to simulate the light source now. the LASER like any other physical entity, can be modeled by its governing equations. In case of LASERS the input is driving current, the output being photons. This system is driven by input output equations which can be simplified to yield the transfer function. This transfer function is used to model the LASER. We make use of models which represent the time variation of the optical power and the chirp of a laser as function of the modulation signal (André *et al.*,1999). To effectively use these models, the physical parameters used in the relations should be clearly understood. For a simple semiconductor laser the dynamics of operations can be studied.

The laser dynamics are modelled by coupled rate equations which describe the relation between the carrier number $N(t)$, the photon density $S(t)$ and the optical phase $f(t)$ (André *et al.*,1999).

The equations are

$$\frac{dN_p(t)}{dt} = \frac{I(t)}{q} - \frac{N_p(t)}{\tau_n} - g_{po} \frac{N_p(t) - N_{pt}}{1 + \epsilon_p S_p(t)} S_p(t) \tag{4}$$

$$\frac{dS_p(t)}{dt} = g_{po} \frac{N_p(t) - N_{pt}}{1 + \epsilon_p S_p(t)} S_p(t) - \frac{S_p(t)}{\tau_p} + \beta_s \frac{N_p(t)}{\tau_n} \tag{5}$$

$$\frac{d\phi(t)}{dt} = \frac{\alpha H}{2} g_{po} [N_p(t) - N_{pt}] \tag{6}$$

which reduce to transfer function of laser as

$$\text{Transfer function of Laser} = \frac{Z}{(z - (2\pi f * 2\pi f)) + j2\pi f Y} \tag{7}$$

where Z and Y are constants that depend on laser parameters. Viz.,

$$Y = g_{po} \frac{S_p}{1 + \epsilon_p S_p} + \frac{1}{\tau_n} - g_{po} \frac{(N_p - N_{pt})}{(1 + \epsilon_p S_p)^2} + \frac{1}{\tau_p} \tag{8}$$

$$Z = g_{po} \frac{S_p}{1 + \epsilon_p S_p} \frac{1}{\tau_p} + (\beta_s - 1) \frac{g_{po}}{\tau_n} \frac{(N_p - N_{pt})}{(1 + \epsilon_p S_p)^2} + \frac{1}{\tau_p \tau_n} \tag{9}$$

Channel model

FSO does not play any part in chaos communication. FSO is just a type of optical communication where free space is the medium i.e., optical fibers are not used. Chaos communication on the other hand is a method of securing data that can be implemented in any mode of communication like radio frequency communication and baseband communication through twisted pairs. Hence FSO has no role in implementation of chaos communication.

We see practically that, an OOK (ON-OFF Keying) system is more robust with regard to atmospheric distortion than a coherent modulation system. This is a direct result of the logic behind the techniques. In OOK schemes the intensity of the output wave is coded (or modified) by the message. OOK is a simple technique analogous to switching on and off a light source. Practically this is what happens in OOK scheme. A logic zero switches OFF the source while a logic high turns it ON. Moreover OOK scheme is intensity dependent. That is when input is high, output is a definite intensity of photons. And when input is low, there is no output i.e., no photons are produced. This particularly helps in free space optical communication systems, because any amount of distortion can only reduce the signal level. But the signal will be present (logic 1) or absent (logic 0) even after atmospheric distortion. As we know atmospheric conditions cause distortions both in the intensity and the phase of a beam, the coherent schemes are not suited. Also that we find OOK very simple to implement both in optical fibers and free space, hence we find a lot of modern optical terminals and networks using OOK setups (Henniger & Wilfert, 2010)

So since we have justified that OOK is the most suited scheme for optical links, all further calculations can be carried out based on the statistics of the received optical power focused on the receiver photodetector (Henniger & Wilfert, 2010). Now for the free space optical

communication we are trying to emulate, we need to address or model the principal atmospheric processes associated that affect the quality of free space communication.

We see that the primary atmospheric processes that affect optical wave propagation are extinction and refractive index turbulence (RIT). These processes lead to attenuation of optical intensity and fluctuations of received optical signal.

Attenuation is caused by microscopic processes like absorption, scattering and refraction of optical signals. These microscopic phenomena are related to gas molecules and aerosols such as fog, snow and rain present at the time of communication. The dominant problem at any problem at hand is a function of distance of communication. For example short distance communication is predominantly affected by fog whereas long distance optical communication faces a sturdy opponent in decreasing signal levels.

At such times signal fluctuations of the received signal P_{RX} can fall below the receiver sensitivity S_{RX} . In such time intervals a so-called "fade" of the signal occurs. Also in case of long distant free space optical links clouds, rain, snow, fog, haze, pollution etc prevent line of sight communication. These factors affect the transmission of a laser beam through the atmosphere. We predominantly concentrate on the signal under clear-sky weather conditions, which is attenuated because of extinction caused by air molecules and aerosols.

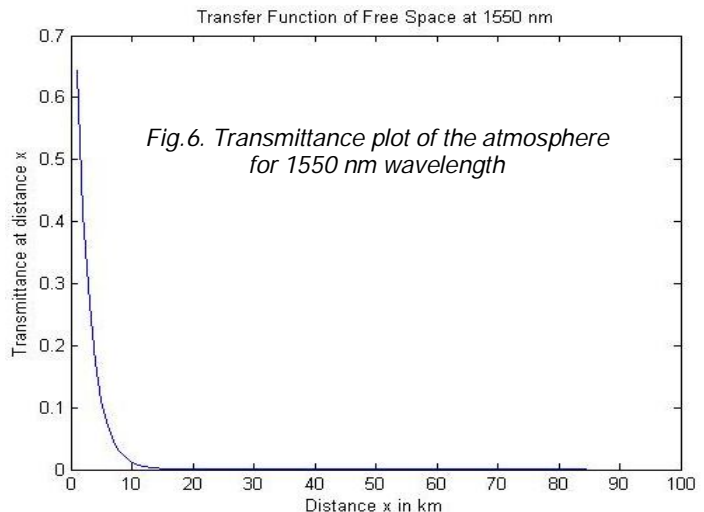
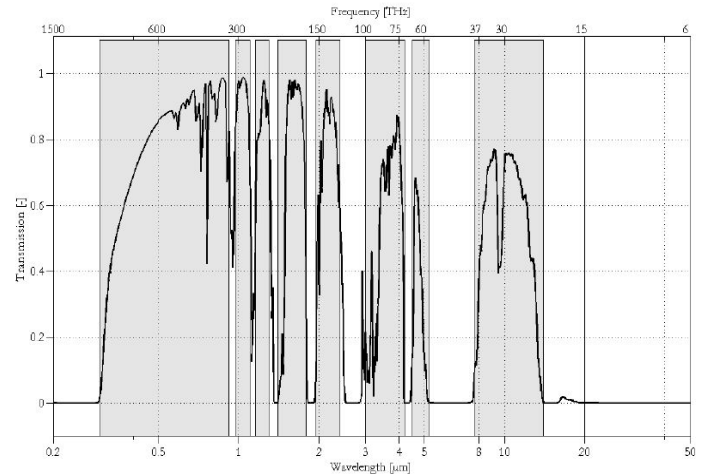
When a laser radiation propagates through a medium, the transmittance T of laser radiation that has propagated over a distance L is described by the Beer's law:

$$T = \exp(-a_e * L[\text{km}]) \quad (10)$$

where the positive extinction coefficient a_e describes the extinction level of the medium. It is usually given in units /km_Beer's law provides the governing expression for determining optical signal power in air medium when the signal has travelled a specific distance in that medium. We know that, the signal under clear-sky weather conditions is attenuated because of extinction caused by air molecules and aerosols. A detailed study of these extinction processes makes us believe that, the extinction is highly wavelength-dependent. Study suggests that the transmission properties of the same set up of atmosphere shows wide variation for varied wavelengths. Fig.5 (Henniger & Wilfert, 2010) gives a description of the atmospheric transmission windows based on extensive evaluation of various data-bases. It can be seen that typical terrestrial communication wavelengths like 808 nm (Si detectors), 1064 nm (Nd-YAG lasers) or 1550 nm (InGaAs detectors, erbium-doped fiber amplifiers) are applicable, whereas 950 nm and 1300 nm are not ideal for FSO systems.

In Fig.5, altitude of 0 km to 120 km as well as the mid-latitude summer atmospheric model are assumed. This figure projects the atmospheric transmittance based

Fig.5. Transmittance plot of the atmosphere for various wavelengths.



on absorption analysis. Atmospheric transmission windows are highlighted in grey colour (Henniger & Wilfert, 2010). Any window of grey colour can be chosen for FSO. However we modelled 8-13μm (the last grey window in the figure) because efficient LASER systems that emit in these regions have already been invented and commercially used. But any LASER emitting in the above grey windows will give a good performance.

In addition to absorption, scattering has also to be taken into account. Scattering can be modelled by the Rayleigh scattering coefficient. Scattering effects are also wavelength dependent in it that, the effects decrease monotonically with wavelength. But it is interesting to note that height also plays a part in it. Also proper care should be taken even in using the optical windows presented above, since there is appreciable extinction possible even in these windows. A rough estimate for the clear-sky extinction is based on the meteorological parameter visibility V . This can be given by the Kruse relation. The Kruse relation, which is modified to reflect the attenuation in decibel per kilometre, is given by Henniger & Wilfert (2010):

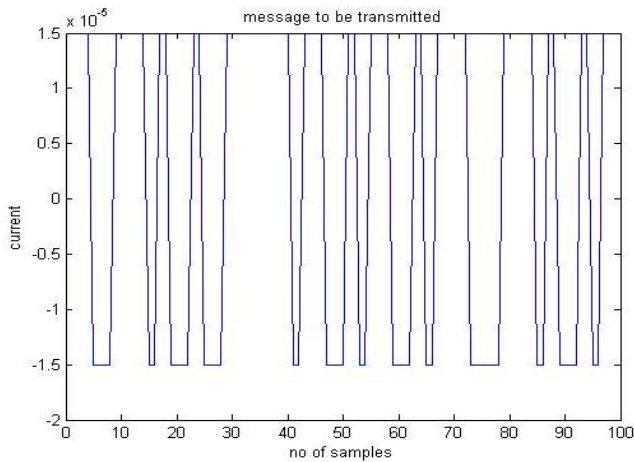
$$A_e[\text{dB/km}] = \frac{17}{V[\text{km}]} \cdot \left(\frac{0.55}{\lambda[\mu\text{m}]} \right)^q \geq 0 \tag{11}$$

where the exponent q is given by

$$\begin{aligned} &1.6 \quad \text{if } V > 50 \text{ km,} \\ &q = 1.3 \quad \text{if } 6 \text{ km} \leq V \leq 50 \text{ km,} \\ &0.585V^{1/3} \quad \text{if } V < 6 \text{ km.} \end{aligned} \tag{12}$$

At 1550 nm, the values calculated were 0.44 dB/km and the corresponding plot is shown in Fig.6.

Fig.7. Transmitted message



Photodetector model

A basic photo diode can be modelled assuming no quantum loss and neglecting all other deviations from ideal behaviour of such a device. The equivalent transfer function can be derived using the same model. It was derived to be,

Transfer function of Photo Diode =

$$\frac{R_i}{(R_d + R_i + j2\pi f C_d R_d R_i)} \tag{13}$$

Since we are concerned about transmitting message at a given data rate, the parameters can be chosen in such a way that the pass band of the device permits frequency corresponding to incoming message frequency (Caffaro & Caffaro, 1993).

Performance

Message retrieval when the system is fully synchronized

A filter designed to be the inverse of channel can be implemented at the receiver's end so that distortion less output can be obtained. But such a filter needs to be adaptive to changes in environmental conditions as the free space is constantly varying channel. However the OOK scheme reduces the need for such filters to be implemented by being robust against distortions due to environmental factors. In this case we simulate a fully synchronized system i.e., the receiver and the transmitter are identical. In other words the system is symmetrical (Liu *et al.*, 2001) thereby the receiver is capable of

producing the same chaos as that produced by the transmitter. Under such conditions the total system function performs close to ideal, showing a very high correlation between given input message at the transmitter and the net output at the receiver. The mean square error between the input and the output is found to be very small. The plot of the same is given in Fig.7 and 8.

Fig.8. Retrieved message with perfectly synchronized transmitter and receiver

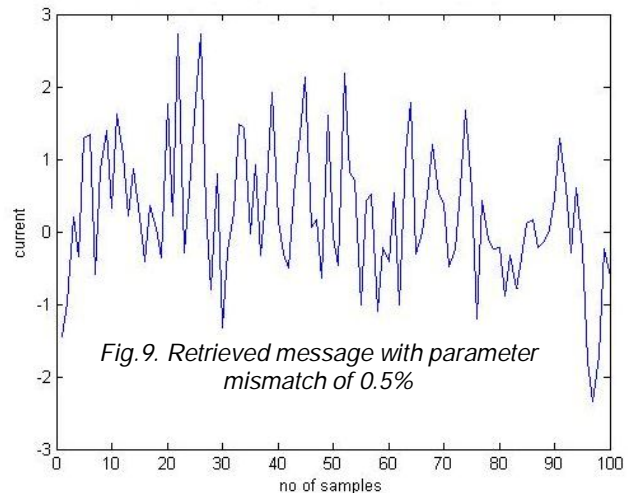
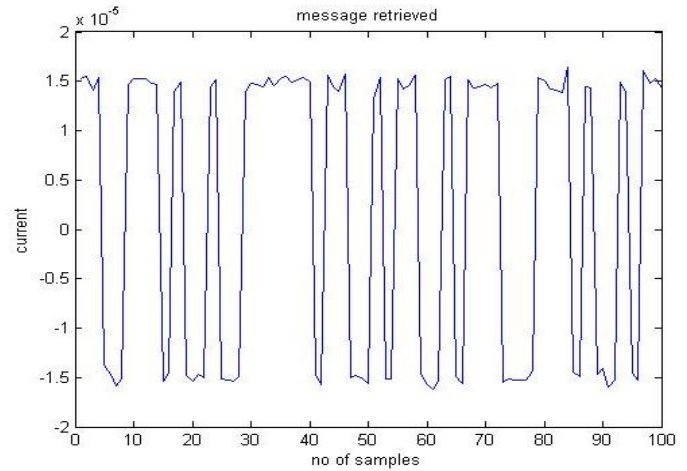


Fig.9. Retrieved message with parameter mismatch of 0.5%

Security offered when the system is not fully synchronized

As we have designed this system for application in secure transmission, we find when the receiver and transmitter are not matched. The system output is unintelligible as shown in Fig.9.

Hence the system is completely secure because even a slight parameter mismatch leads to a wide divergence in the generated chaos which leads to a completely unintelligible message being retrieved at the receiver

Conclusion

We simulated a chaotic optical communication system by modeling the individual components in it. Upon executing such a system, expected results are obtained

when the whole system is completely synchronized. However, introduction of a small mismatch produces totally unintelligible results. Hence, this is a good method for secure communication. But this method has two disadvantages. Synchronisation needs to be very precise: even the smallest error between the chaos generated at the Transmitter and that generated at the Receiver can be expected to grow exponentially. Second, since an optical system consists of components viz., laser, a channel and a photodetector all of whose performance depends on temperature of operation. Physically there is no difference between the normal LASER and the one we have designed. However for computational simplicity we have assumed quantum efficiency equal to 100%, which is practically not possible. This is the only compromise we have made. But this will not affect system performance because of a Quantum Efficiency of less than 100%, only the number of photons emitted per injected electron decreases. But since we use OOK scheme, the number of photons released is not a concern because we bother about the presence (logic high) or absence of photons (logic low) and not their count. Hence, proper temperature compensation must be established; else the error introduced is increased at every stage leading to decreased system performance. However, for encryption of very sensitive information where cost might be a secondary factor, this method is very safe.

References

1. André PS, Nolasco Pinto A, Pinto JL and da Rocha F (1999) Extraction of LASER rate equations parameters. *SPIE*. 3572, 141-146.
2. Caffaro MAG and Caffaro MG (1993) A new methodology for the analysis of the stability of optical solitary waves in solids. *Optik*. 93, 183-186.
3. Claudio R. Mirasso, Ingo Fischer, Michael Peil and Laurent Larger (2003) Optoelectronic devices for optical chaos communications. *Proc. of SPIE*, 5248, 24.
4. Éric Genin, Laurent Larger, Jean-Pierre Goedgebuer, Min Won Lee, Richard Ferrière, and Xavier Bavard (2004) Chaotic oscillations of the optical phase for multi-GigaHertz bandwidth secure communications. *IEEE J. Quantum Electronics*. 40 (3), 294-298.
5. Grado Caffaro MA and Grado Caffaro M (1993) New results on bandwidth of GaAs PIN photodiodes. *Active & Passive Electronic Components*. 16, 23-27.
6. Hennes Henniger and Otakar Wilfert (2010) An introduction to free-space optical communication. *Radio Engg*. 19 (2), 203-212.
7. Larger L, Udaltsov VS and Poinot S and Genin E (2005) Optoelectronic phase chaos generator for secure communication. *J. Optical Technol*. 72(5), 378-382.
8. Liu Y, Chen HF, Liu JM, Davis P and Aida T (2001) Communication using synchronization of optical-feedback induced chaos in semiconductor lasers. *IEEE Transact. on Signals & Systems-I: Fundamental Theory & Appl*. 48 (12), 1484-1490.
9. Suzuki K and Imai Y (2003) Message modulation type secure communication characteristics using optical fiber ring resonator chaos, *THP-(5)-8*. IEEE. pp: 534.
10. Valerio Annovazzi-Lodi, Giuseppe Aromataris, Mauro Benedetti and Sabina Merlo (2008) Secure chaotic transmission on a free-space optics data link. *IEEE J. Quantum Electronics*. 44 (11), 1089-1095.