We propose and experimentally demonstrate a new chaos based opto-electronic secure communication system using voltage control oscillator. The chaotic signal has been generated using a modified electronic circuit of the logistic map. The output of the chaos generator is translated to a chaotically varying instantaneous frequency of the voltage controlled oscillator (VCO). The proposed technique encodes the signal using this chaotically varying instantaneous frequency. The proposed technique has been demonstrated by using an optical fiber as a communication channel. Experimental results have been presented as a proof of concept.

INTRODUCTION

The transmission of huge amount of data has led to remarkable research efforts in the area of data security. In the past decade, several algorithms and architectures for optical image-encryption and security systems have been proposed (B. Javidi, 2005; P. Refregier, and B. Javidi 1995; M. Singh, A. Kumar, and K. Singh 2008; Z. Liu, J. Dai, X. Sun, and S. Liu 2009; C. C. Laborde, R. Duchowicz, R. Torroba, and E.E. Sicre 2008; H. Li 2009; X. Li, and D. Zhao; M. Ouhsain, and A.B. Hamza 2009) in which, we desire to encode information in such a way that, even if it is viewed or recorded, only the use of the correct key would fetch the correct information for the guaranteed privacy. Chaos has the potential to guarantee privacy for transmitted signal due to its attractive properties (G. James, 1988; K.T. Alligood, T.D. Sauer, and J.A. Yorke. 2001; R.C. Hilborn. Chaos and nonlinear dynamic, 2000). Chaotic waveforms have been generated using different hardware systems ([M. Sunel, 2006; I.C. Canton, E. C. Canton, J.S. Murgui, and H.C. Rosu, 2008; K. Murali, Sudeshna Sinha, William L. and Ditto, 2003). Their attractive features are their broadband spectrum and the possibility of synchronizing them. The hardware-oriented (R.A. Gayakward, 2004; B.P. Lathi, 2005) secure system could guarantee greater privacy than that obtained with conventional software-oriented cryptography (A. Argyris, D. Syvridis, L. Largar, V. A. Lodi, P. Colet, I. Fischer, J.G. Ojalvo, C.R. Mirasso, L. Pesquera, and K.A., 2005). Recently chaotic based signal have been utilized to encode information and provide added security (A. Argyris, D. Syvridis, L. Largar, V. A. Lodi, P. Colet, I. Fischer, J.G. Ojalvo, C.R. Mirasso, L. Pesquera, and K.A., 2005; C.R. Mirasso, I. Fischer, and L. Larger).

In this paper, we propose and experimentally demonstrate a new chaos based opto-electronic secure communication system using VCO. The chaotic signal has been generated using a modified electronic circuit of the logistic map. The output of the chaos generator is translated to a chaotically varying instantaneous frequency of the voltage controlled oscillator. The proposed technique encodes the signal using this chaotically varying instantaneous frequency. The proposed technique has been demonstrated by using an optical fiber as a communication channel. Experimental results have been presented as a proof of concept. The proposed technique is different from the earlier techniques. In the previous techniques, encryption has been performed when signal is transformed from one domain to another domain (the signal has been transformed using a transform to the frequency domain by using Fourier transform (FT) (B. Javidi, 2005; X. Li, and D. Zhao-8). Chaotic signal has chaotic variation in both the amplitude and the instantaneous frequency. In all the earlier proposed techniques, masking (encryption) of the message has been performed by using the chaotic variation in amplitude of the chaotic signal (A. Argyris, D. Syvridis, L. Largar, V.A. Lodi, P. Colet, I. Fischer, J.G. Ojalvo,
C.R. Mirasso, L. Pesquera, and K.A. 2005; -B. Cuenot, L. Larger, J.-P. Goedgebuer, and William T. Rhodes, 2001; L. Larger, and J-P Goedgebuer, 2004; L. Larger, J-P Goedgebuer, and V. Udaltsov, 2004; K. Suzuki, and Y. Imai, 2006; C.R. Mirasso, I. Fischer, and L. Larger). In the proposed technique, the VCO output is not the FT of chaotic waveform generated by the chaos generator but the VCO output remains in the temporal domain i.e. the domain does not change for the encryption process. The masking (encryption) of the message has been done by using the chaotic variation in instantaneous frequency of the chaotic signal.

2. Voltage Controlled Oscillator:
An oscillator whose frequency can be controlled by an external voltage is a VCO (R.A. Gayakward, 2004 ; B.P.Lathi, 2005). In a VCO, the oscillation frequency varies linearly with the input voltage is \(f_o(t)\). Its output is a sinusoid of frequency \(\omega\) given by

\[
\omega(t) = \omega_c + ce_o(t)
\]

where \(\omega_c\) is a constant of the VCO and \(c\) is the free-running frequency of the VCO (the VCO frequency when \(e_o(t) = 0\)). The multiplier output is further low pass filtered by the loop filter and then applied to the input of the VCO. This voltage changes the frequency of the oscillator and keeps the loop locked. This function is achieved in the VCO. VCO is also called a voltage to frequency converter. Phase locked loop (PLL) serves as a VCO demodulator. The PLL can be used to track the phase and the frequency of the carrier component of an incoming signal. It is, therefore, a useful device for synchronous demodulation of amplitude modulation (AM) signals with suppressed carrier or with a little carrier (the pilot). A PLL has three basic components. First is a VCO, second is, a multiplier, serving as a phase detector or a phase comparator and third is a loop filter. The operation of the PLL is similar to that of a feedback system. The central frequency of the PLL is determined by the free-running frequency of the VCO, which is given by the equation

\[
f_{out} = \frac{1.2}{4RC}
\]

where \(R\) and \(C\) are the resistor and capacitor. The lock range \(f_L\) and capture range \(f_c\) of the PLL are given by

\[
f_L = \frac{8f_{out}}{V}
\]

\[
f_c = \left[\frac{f_L}{(2\pi)(3.6)(10^8)(C)}\right]^{1/2}
\]

where \(f_{out}\) is the free running frequency of VCO and \(V\) is the supply voltage. The lock range usually increases with an increase in the input voltage but decreases with an increase in the supply voltage.

3. Chaos Function:
Logistic map [10-12] is a chaotic map. Chaotic maps generate chaotic signals which have properties such as the wideband wave form does not repeat itself. It has noise like appearance and is very sensitive to the initial conditions. These random iterative values are limited between bounds. The logistic map is used for our study and is defined as

\[
f(x) = \lambda x (1 - x)
\]
This function is bounded for $0 < \lambda < 4$. The iterative form of this function is written as

$$x_{n+1} = \lambda x_n (1 - x_n)$$  \hspace{1cm} (6)

with $x_0$ as the initial value. This chaotic map is used to generate the chaotic signal.

The encryption process and the decryption process of the proposed technique are shown in Fig. 1. Let $S(t)$ be the input signal and the $C(t)$ be the chaotic signal, where $C(t)$ is the random waveform generated by the electronic circuit of the logistic map. Both the input signal and the chaotic signal are processed by the VCO. The VCO converts the input signal into another signal $S_{VCO}(t)$ of varying instantaneous frequency. Similarly, the chaotic signal is converted into a signal $C_{VCO}(t)$ with chaotically varying instantaneous frequency. Both are then multiplied together to give the encrypted signal $E(t)$. It is given by

$$E(t) = C_{VCO}(t) \times S_{VCO}(t)$$  \hspace{1cm} (7)

The decryption process is the inverse of the encryption process. $C_{VCO}(t)$ is multiplied with $E(t)$ and then the VCO demodulation operation is performed. The obtained signal is the decrypted signal which is expressed as $D(t)$ and is given by

$$D(t) = \text{VCOdemodulation}[E(t) \times C_{VCO}(t)]$$  \hspace{1cm} (8)

**Fig. 2:** Modified circuit diagram for logistic map.

The modified circuit diagram of the logistic map is shown in Fig. 2. Some modifications have been introduced between the present circuit diagram of the logistic map and the earlier proposed circuit diagram of the logistic map (M. Suneel, 2006). These modifications are as follows. There is an option to change the seed value of the electronic circuit of the logistic map. Every time the seed value can be changed by using the variable resistance at pin no. 6 of the second multiplier. IC 741 (single output general-purpose operational amplifier) is used to design the electronic circuit of subtractor and amplifier respectively. LF633 IC is used to design the electronic circuit of first and second multipliers respectively. A simple circuit using single LF398 IC (sample and hold IC) is used to iterate the loop of the electronic circuit of logistic map. Every time the seed value can be changed by using the variable resistance at pin no. 6 of the second multiplier. IC 741 (single output general-purpose operational amplifier) is used to design the electronic circuit of subtractor and amplifier respectively. LF633 IC is used to design the electronic circuit of first and second multipliers respectively. A simple circuit using single LF398 IC (sample and hold IC) is used to iterate the loop of the electronic circuit of logistic map. Here $R_1 = R_2 = R_3 = 2.2K\Omega$ and $R_4 = R_5 = R_6 = R_7 = 22K\Omega$. IC 633 is used to implement $M_1$ and $M_2$. Here $C_1 = C_2 = C_3 = C_4 = 0.1 \mu F$. Here $C_5 = 0.1 \mu F$. $R_{13}$ and $R_{14}$ are the variable resistance of $5K\Omega$. The trigger of the sample-and-hold circuit is a TTL-compatible square-wave generated by using the function generator. Here $V_{cc} = +15V$ and $V_{EE} = -15V$. Frequency of the trigger signal is equal to $300Hz$ and amplitude is equal to $5Volt$. For VCO and PLL, IC LM566CN serves as the VCO and IC LM565CN serves as the PLL respectively. In the opto-electronic implementation of the encryption and the decryption technique, the optical fiber has been used to demonstrate the proposed technique.

**Experimental Results:**

Experimental results have been presented to validate the proposed technique. Electronic circuit of the logistic map has been designed to generate the chaotic signal. The input signal is a sinusoidal wave having a amplitude of $0-5V$ and frequency of $300Hz$. Trigger pulse for the logistic map circuit is TTL pulse of amplitude $0-5V$ and frequency $300Hz$. Amplitude of the chaotic signal is $1volt$. The amplitude of the VCO output when input signal is input of the VCO is kept in between $-1V$ to $1V$. The amplitude of the VCO output when chaotic
The input signal is input of the VCO is kept in between -1V to 1V. The frequency of the input signal and the trigger signal is kept equal. TTL pulse and the input signal is given by function generator.

The experimental results for the encryption and the decryption process are given in Fig. 3. The input signal, a sinusoid, is given in Fig. 3(a). The chaotic signal generated by our circuit is shown in Fig. 3(b). The combined signal of the input and the chaotic signal is given in Fig. 3(c). (d) the encrypted signal (signal after performing PPM and at the transmitter end of the HFBR) is shown in Fig. 3(d). Finally the decrypted signal is shown in Fig. 3(e).

**Conclusion:**

In conclusion, we propose and experimentally demonstrate a new chaos based opto-electronic secure communication system using VCO. The proposed technique is different from the previous techniques. In the previous techniques, the encryption is carried out by first transforming the signal from one domain to another domain. Masking is done by using the chaotic variation in the amplitude of the chaotic signal. In the proposed technique, the encryption has been performed in the same domain (time domain) and it is first time that the masking has been done by using the chaotic variation of the instantaneous frequency of the chaotic signal. A modified electronic circuit has been used to generate the chaotic signal. The proposed technique has been validated by using an optical fiber as a communication channel.

**Fig. 3:** The experimental results (a) The input signal, (b) the chaotic signal, (c) the combined signal of the input and the chaotic signal, (d) the encrypted signal (signal after performing PPM and at the transmitter end of the HFBR), and (e) the decrypted signal.
REFERENCES


