Secure Communication using Compound Signal from Generalized Synchronizable Chaotic Systems

K.Murali and M. Lakshmanan

Centre for Nonlinear Dynamics, Department of Physics, Bharathidasan University, Tiruchirappalli - 620 024, India

By considering generalized synchronizable chaotic systems, the drive-auxiliary system variables are combined suitably using encryption key functions to obtain a compound chaotic signal. An appropriate feedback loop is constructed in the response-auxiliary system to achieve synchronization among the variables of the drive-auxiliary and response-auxiliary systems. We apply this approach to transmit analog and digital information signals in which the quality of the recovered signal is higher and the encoding is more secure.

Several recent studies have shown the possibility of synchronizing chaotic systems and its usefulness in secure communications[1-14]. Among the available chaos synchronization schemes, in the first method due to Pecora and Carroll[2] a stable subsystem of a chaotic system is synchronized with a separate chaotic subsystem under suitable conditions. This method has been further extended to cascading chaos synchronization with multiple stable subsystems[1-5]. The second method to achieve chaos synchronization is due to the approach of one-way coupling, in which two identical chaotic systems are synchronized without requiring to construct any stable subsystem[7,8]. In both these approaches only one chaotic signal from the drive system is utilized to drive the response systems. These are the most frequently studied schemes where the complete system consists of coupled identical subsystems[1-8]. In these cases the synchronization appears as an actual equality of the corresponding variables of the coupled systems as they evolve in time. This type of synchronization is now called the *conventional synchronization*(**CS**)[15-20]. However a more complicated situation arises when *coupled nonidentical chaotic systems* are considered. This kind of problem has been recently reported by Rulkov *et al.*[15] in which a generalization of synchronization for unidirectionally coupled systems was proposed, where two systems are called synchronized if a (static) functional relation exists between the states of both the systems. The resulting synchronization is called *generalized synchronization*(**GS**)[15-17,19,20] and a general theory for **GS** of unidirectionally coupled systems was developed in [15]. Recently in ref.[18] the concept of synchronization and communication through compound chaotic signal generated using *encryption key functions* have been reported. This approach can be further extended by including different auxiliary chaotic systems both at the drive and response systems so that both **CS** and **GS** are used where all the *drive-auxiliary system* variables are combined suitably so that a compound chaotic drive signal is so produced to drive the *response-auxiliary system*. A feedback loop in the *response-auxiliary system* is constructed appropriately to achieve synchronization among the variables of the drive and response systems. The importance of the present method is that both the drive and response systems are totally unaltered(unlike the standard available method for **GS**) and the arrangement can be easily implemented in practical situations for communications. Also the transmitted compound chaotic signal looks more complex depending upon the type of *encryption key function* used, thereby improving the security as well.

The present suggested method of chaos synchronization can be described as follows. Let us consider the following form of the drive-auxiliary system equations:
drive:

$$\dot{\mathbf{x}} = \mathbf{f}(\mathbf{x}) + \epsilon(v(t) - x_j(t)), \tag{1}$$

$$\dot{\mathbf{y}} = \mathbf{f}(\mathbf{y}) + \epsilon(u(t) - y_j(t)), \tag{2}$$

auxiliary system:

$$\dot{\mathbf{z}} = \mathbf{g}(\mathbf{z}) + \epsilon(y_j(t) - z_j(t)), \tag{3}$$

where $\mathbf{x}$ and $\mathbf{y}$ are identical chaotic systems and $\mathbf{z}$ is a different chaotic system(so called auxiliary system) unidirectionally driven by the chaotic variable $y_j(t)$. If $v(t) = y_j(t)$ and $u(t) = x_j(t)$ then Eqs.(1) and (2) are two identical chaotic systems mutually coupled together with the signals at the jth component. This kind of mutually coupled chaotic systems have been well studied[9]. Here two self-synchronizable chaotic systems (1) and (2) are used for experimental operational convenience, which then are to be used for secure signal transmission applications. Due to the present simple set-up, the information signal can easily be injected as a voltage source experimentally to the chaotic carrier for secure communication. We have infact explicitly shown numerically the applicability of this kind of set-up in the following discussions.

Now the two mutually coupled self-synchronized systems (1) and (2) are considered together with the one-way coupled auxiliary system (3) as a single *drive* system. The concept of chaos synchronization through $drive - response$

formalism is then established by considering the *response* system equations as
response:

$$\dot{\mathbf{y}}_\mathbf{r} = \mathbf{f}(\mathbf{y}_\mathbf{r}) + \epsilon_r(v_r(t) - (y_r)_j(t)). \tag{4}$$

auxiliary system:

$$\dot{\mathbf{z}}_\mathbf{r} = \mathbf{g}(\mathbf{z}_\mathbf{r}) + \epsilon_r((y_r)_j(t) - (z_r)_j(t)). \tag{5}$$

Here $\mathbf{y}_\mathbf{r}$ is the copy of $\mathbf{x}$ or $\mathbf{y}$ and is driven by the signal $v_r(t) = v(t) = y_j(t)$ through one-way coupling[7,8] and $\mathbf{z}_\mathbf{r}$ is the copy of $\mathbf{z}$. Here ϵ_r is the one-way coupling parameter. If the maximal Lyapunov exponent of (4) is negative under the influence of the chaotic signal $v_r(t)$ added to the jth component of the response system vector field $\dot{\mathbf{y}}_\mathbf{r} = \mathbf{f}(\mathbf{y}_\mathbf{r})$, then $\| \mathbf{y}_\mathbf{r} - \mathbf{y} \| \to 0$ for $t \to \infty$. Also if the maximal Lyapunov exponent of (5) is negative under the influence of the chaotic signal $(y_r)_j(t)$ added to the jth component of the auxiliary system vector field $\dot{\mathbf{z}}_\mathbf{r} = \mathbf{g}(\mathbf{z}_\mathbf{r})$, then $\| \mathbf{z}_\mathbf{r} - \mathbf{z} \| \to 0$ for $t \to \infty$. Synchronization between systems (1) and (2) occurs if the dynamical system describing the evolution of the difference $\mathbf{e} = \mathbf{x} - \mathbf{y}$,

$$\dot{\mathbf{e}} = \dot{\mathbf{x}} - \dot{\mathbf{y}}, \tag{6}$$

possesses a stable fixed point at the origin $\mathbf{e} = \mathbf{0}$ and synchronization between (4) and (2) occurs if

$$\dot{\mathbf{e}}_\mathbf{y} = (\dot{\mathbf{y}}_\mathbf{r} - \dot{\mathbf{y}}), \tag{7}$$

possesses a stable fixed point at the origin $\mathbf{e}_\mathbf{y} = \mathbf{0}$. Also synchronization between (5) and (3) occurs if

$$\dot{\mathbf{e}}_\mathbf{z} = (\dot{\mathbf{z}}_\mathbf{r} - \dot{\mathbf{z}}), \tag{8}$$

possesses a stable fixed point at the origin $\mathbf{e}_\mathbf{z} = \mathbf{0}$. This can be further proved by using (global) Lyapunov functions[3]. In this kind of setup **CS** occurs between $\mathbf{x}$ & $\mathbf{y}$, $\mathbf{y}_\mathbf{r}$ & $\mathbf{y}$ and $\mathbf{z}_\mathbf{r}$ & $\mathbf{z}$. However **GS** between $\mathbf{y}$&$\mathbf{z}$ occurs since there is the **CS** between $\mathbf{z}$ and $\mathbf{z}_\mathbf{r}$[15-17,20]. However, it is not necessary that only one of the drive variables alone be used for synchronization with the response system($v_r(t) = y_j(t)$). One can also combine and modify the drive signal appropriately, and then undo the transformation at the response system for synchronization[18,19]. Instead of using one drive signal variable, one can transform the drive-auxiliary system variables by appropriate linear or nonlinear combinations(which can be treated as **encryption key function**) to produce a compound chaotic signal for use as the drive signal for synchronization with the response-auxiliary systems. A suitable feedback loop can be deviced in the response-auxiliary system to achieve synchronization among the variables of the drive and response systems. The arrangement is illustrated schematically in Figure 1.

We have used the well-known Chua's circuit[9,10] as the drive system. We have considered the auxilary systems as (i) Murali-Lakshmanan-Chua(MLC) circuit[1,21] for the non-autonomous case and (ii) Lorenz system for the autonomous case to demonstrate the above scheme of chaos synchronization. The first example consists of the the model equations for the Chua's circuit and MLC circuit which are represented as
drive:

$$\dot{x}_1 = \alpha((x_2 - x_1 - g_1(x_1)) + \epsilon(v(t) - x_1)), \tag{9}$$
$$\dot{x}_2 = x_1 - x_2 + x_3, \tag{10}$$
$$\dot{x}_3 = -\beta x_2, \tag{11}$$
$$\dot{y}_1 = \alpha((y_2 - y_1 - g_1(y_1)) + \epsilon(u(t) - y_1)), \tag{12}$$
$$\dot{y}_2 = y_1 - y_2 + y_3, \tag{13}$$
$$\dot{y}_3 = -\beta y_2, \tag{14}$$

non-autonomous auxiliary system:

$$\dot{z}_1 = z_2 - g_2(z_1) + \epsilon_r(y_1 - z_1), \tag{15}$$
$$\dot{z}_2 = -\sigma z_2 - z_1 + F sin(\omega t), \tag{16}$$

where $g_1(x) = b_1 x + 0.5(a_1 - b_1)(|x+1| - |x-1|)$ and $g_2(x) = b_2 x + 0.5(a_2 - b_2)(|x+1| - |x-1|)$ and $a_1 = -1.27, b_1 = -0.68, a_2 = -1.02, b_2 = -0.55, \sigma = 1.015, F = 0.15, \omega = 0.75$, α=10.0 and β=14.87. If $v(t) = y_1$ and $u(t) = x_1$ then for appropriate values of mutual coupling parameter ϵ(ϵ=1.3), the above system of equations (9-14) self-synchronizes.

After synchronization x_1=y_1,x_2=y_2, and x_3=y_3. Let us now choose an appropriate drive encryption key function.
drive encryption key:

$$K_d = h(y_1, y_2, y_3, z_1, z_2), \tag{17}$$

so that we can generate a sufficiently complicated compound chaotic signal to be transmitted. The form of the *encryption key function* is entirely within our choice. We may choose the function as $z_1, z_1^2, y_2z_1^2, y_2^2z_1, y_2y_3z_1z_2, y_2^3z_1$,... . Then the *encryption key function* is combined with the signal from the drive to generate the compound drive signal for transmission.
compound drive signal:

$$d(t) = v(t) + K_d = y_1 + h, \tag{18}$$

Then the response system equations are
response:
response encryption key:

$$K_r = h(y_{1r}, y_{2r}, y_{3r}, z_{1r}, z_{2r}) \equiv h_r, \tag{19}$$

regenerated drive signal:

$$v_r(t) = d(t) - K_r = d(t) - h_r, \tag{20}$$

$$\dot{y}_{1r} = \alpha((y_{2r} - y_{1r} - g_1(y_{1r})) + \epsilon_r(v_r(t) - y_{1r})), \tag{21}$$
$$\dot{y}_{2r} = y_{1r} - y_{2r} + y_{3r}, \tag{22}$$
$$\dot{y}_{3r} = -\beta y_{2r}. \tag{23}$$

auxiliary system:

$$\dot{z}_{1r} = z_{2r} - g_2(z_{1r}) + \epsilon_r(y_{1r} - z_{1r}), \tag{24}$$
$$\dot{z}_{2r} = -\sigma z_{2r} - z_{1r} + F sin(\omega t). \tag{25}$$

In the following we first demonstrate the effectiveness of our model analytically and numerically for the specific choice $h = z_1$ and $h_r = z_{1r}$. Then we point out the applicability for more complicated forms of h numerically. The difference system($\mathbf{e} = \mathbf{x} - \mathbf{y}$) of Eqs.(9-11) and Eqs.(12-14) is

$$\dot{e}_1 = \alpha((e_2 - e_1 - p_i e_1) - 2\epsilon e_1), \tag{26}$$
$$\dot{e}_2 = e_1 - e_2 + e_3, \tag{27}$$
$$\dot{e}_3 = -\beta e_2, \tag{28}$$

where $p_i = a_1$ or b_1(i=1 or 2) which is determined from $g_1(x)$[9]. It is easy to prove that the temporal derivative of the positive definite Lyapunov function

$$E = (\beta/2)e_1^2 + (\alpha\beta/2)e_2^2 + (\alpha/2)e_3^2, \tag{29}$$

is strictly negative,

$$\dot{E} = \beta e_1\dot{e}_1 + \alpha\beta e_2\dot{e}_2 + \alpha e_3\dot{e}_3, \tag{30}$$
$$= -\alpha\beta(e_1 - e_2)^2 - \alpha\beta(a_1 + 2\epsilon)e_1^2 < 0 \tag{31}$$

for all e_1, e_2, e_3 when $\epsilon > -a_1/2$. (Note that $a_1 < b_1 < 0$ and $a_1 = -1.27$)[9].

Also the difference system of Eqs.(12-16) and Eqs.(21-25) for the specific choice $h = z_1$ and $h_r = z_{1r}$ is given as

$$\dot{e}_{y1} = \alpha((e_{y2} - e_{y1} - p_i e_{y1}) - \epsilon_r(e_{y1} + e_{z1})), \tag{32}$$
$$\dot{e}_{y2} = e_{y1} - e_{y2} + e_{y3}, \tag{33}$$
$$\dot{e}_{y3} = -\beta e_{y2}, \tag{34}$$
$$\dot{e}_{z1} = e_{z2} - q_i e_{z1} + \epsilon_r(e_{y1} - e_{z1})), \tag{35}$$
$$\dot{e}_{z2} = -\sigma e_{z2} - e_{z1}, \tag{36}$$

where $q_i = a_2$ or b_2(i=1 or 2) which is determined from $g_2(x)$. Here $e_{y1} = (y_{1r} - y_1), e_{y2} = (y_{2r} - y_2)$, $e_{y3} = (y_{3r} - y_3)$, $e_{z1} = (z_{1r} - z_1)$ and $e_{z2} = (z_{2r} - z_2)$.

It is easy to prove that the temporal derivative of the positive definite Lyapunov function

$$E = (\beta/2)e_{y1}^2 + (\alpha/2)e_{y3}^2 + (\alpha\beta/2)(e_{y2}^2 + e_{z1}^2 + e_{z2}^2), \tag{37}$$

is strictly negative,

$$\begin{aligned}\dot{E} &= \beta e_{y1}\dot{e}_{y1} + \alpha\beta e_{y2}\dot{e}_{y2} + \alpha e_{y3}\dot{e}_{y3} \\ &\quad + \alpha\beta e_{z1}\dot{e}_{z1} + \alpha\beta e_{z2}\dot{e}_{z2}, \qquad (38)\\ &= -\alpha\beta[(e_{y1} - e_{y2})^2 + (a_1 + \epsilon_r)e_{y1}^2 \\ &\quad + (a_2 + \epsilon_r)e_{z1}^2 + \sigma e_{z2}^2] < 0, \qquad (39)\end{aligned}$$

for all $e_{y1}, e_{y2}, e_{y3}, e_{z1}$ and e_{z2} when $\epsilon_r > -a_1$. Further the conditional Lyapunov exponents of the response system Eqs.(21-23) for the given value of one-way coupling parameter ϵ_r can be computed through numerical simulations. For ϵ_r=1.3, the conditional Lyapunov exponents are $(-0.2019, -0.2017, -12.43)$. Figures 2(a-d) depict the phase-portraits in the (y_2-y_1)-plane, (z_2-z_1)-plane, (z_1-y_1)-plane and ($d(t)$-y_1)-plane respectively. The qualitative shape of the attractor in Fig.2(d) depends upon the type of *encryption key*. As the maximal conditional Lyapunov exponent is negative, synchronization between drive and response systems is achieved as shown in Figs.3(a-b) for ϵ_r=1.3. Also the conditional Lyapunov exponents of the *auxiliary systems* (15-16) and (24-25) are calculated as $(-0.8584, -0.855, 0.0)$.

The above scheme of synchronization can be used to construct transmitter-receiver systems for encoding and masking information data signals. To send the information signal $s(t)$ from the transmitter to receiver using the familiar *chaos signal masking technique*[1,3-6,18], now the signals $v(t)$ and $u(t)$ are modified as $v(t) = y_1 + s(t)$ and $u(t) = x_1 + s(t)$ respectively. The significance of this type of encoding the message signal $s(t)$ is not only that it is added just to a chaotic carrier but it also simultaneously drives the self-synchronizing transmitter dynamical system. Such an encoding procedure ensures security and also avoids the typical distortion errors that occur in almost all previous communication schemes based on chaos synchronization[10]. By employing this scheme, signal is recovered at the response system Eqs.(19-25) as
recovered signal:

$$r(t) = v_r(t) - y_{1r} = s(t). \tag{40}$$

Figure 3(c) and 3(d) show the numerical simulation results of the transmitted compound chaotic signal $d(t)$ and the recovered signal $(sinewave, 0.02\sin 0.5t)$ respectively.

In order to demostrate the signal transmission applications using nonlinear *encryption key functions*, in the following we have used $K_d = h = y_2 z_1$. Then the *compound drive signal* is represented as $y_1 + y_2 z_1$ and the *regenerated drive signal* at the response system equations(21-25) is given as $v_r(t) = d(t) - y_{2r}z_{1r}$. Figures 4(a-c) depict the phase-portrait in $(d(t) - y_1)$-plane for ϵ_r=1.3, the transmitted compound chaotic signal $d(t)$ and the recovered information signal (*sinewave*, 0.03sin0.2t) respectively. Also Figures 5(a-c) show the numerical simulation results of the digital information signal $s(t)$, the transmitted compound chaotic signal $d(t)$ and the recovered digital information signal $r(t)$ for ϵ_r=1.3 respectively for the choice of $h = y_2 z_1$.

In the above analysis we have used the auxiliary system as a nonautonomous system. One can as well use an autonomous auxiliary system. In the following we choose the auxiliary system as the Lorenz system. The drive equations are the same as Eqs.(9-14) and also the response equations (21-23). Now the autonomous auxiliary system is considered as the Lorenz system driven by the chaotic signal y_1 (from Eqs.(12-14)) and the governing model equations are represented as
autonomous auxiliary system:

$$\dot{z}_1 = -\sigma(z_1 - z_2), \tag{41}$$

$$\dot{z}_2 = r y_1 - z_2 - y_1 z_3, \tag{42}$$

$$\dot{z}_3 = y_1 z_2 - b z_3, \tag{43}$$

drive encryption key:

$$K_d = h(z_1, z_2) = z_1, \tag{44}$$

compound drive signal:

$$d(t) = v(t) + K_d = y_1 + z_1, \tag{45}$$

Then the response system equations are
response:
response encryption key:

$$K_r = h(z_{1r}, z_{2r}) = z_{1r}, \tag{46}$$

regenerated drive signal:

$$v_r(t) = d(t) - K_r = d(t) - z_{1r}. \tag{47}$$

auxiliary system:

$$\dot{z}_{1r} = -\sigma(z_{1r} - z_{2r}), \tag{48}$$
$$\dot{z}_{2r} = ry_{1r} - z_{2r} - y_{r1}z_{3r}, \tag{49}$$
$$\dot{z}_{3r} = y_{1r}z_{2r} - bz_{3r}, \tag{50}$$

.

Here y_{1r} is the signal generated from Eqs.(21-23). Figures 5(a-b) show the phase-portrait in the $(z_3 - z_2) - plane$ and $(d(t) - y_1)$-plane respectively for ϵ_r=1.3, σ=10, r=28 and b=2.666. Further by using this model (Eqs.(41-50)) for secure signal communications, Figure 6(a-c) depict the numerical simulation results of the difference signal $(z_{1r} - z_1)$, transmited compound chaotic signal $d(t)$ and the recovered analog signal(0.02sin0.5t) respectively. As mentioned earlier one can also use more complicated encryption key functions without any difficulty. We also note here that recently, Chua's circuits(without auxiliary systems) represented by Eqs.(9-14,20-23) have been used to demonstrate experimentally the present scheme of secure communication for analog and digital signals through compound chaotic signal(generated with suitable encryption key functions)[22].

In conclusion, we have presented a procedure of achieving an efficient synchronization using a compound chaotic signal generated from generalized synchronizable chaotic systems. By considering suitable *encryption key functions* a compound drive chaotic signal is produced and with appropriate feedback-loop at the receiver, synchronization among the variables of the drive and response has been established. Also, its application in secure communications of analog and digital information signals has been demonstrated and the information signals have been recovered perfectly. Due to the present scheme of efficient encoding of message signals with suitable encryption key functions the compound chaotic signal looks more complex thereby improving the security of the transmitted signal.

This work has been supported through a research project by the Department of Science and Technology, Government of India.

---

[1] M.Lakshmanan and K.Murali, *Chaos in Nonlinear Oscillators: Controlling and Synchronization* (World Scientific, Singapore 1996).
[2] L.Pecora and T.Carroll, Phys.Rev.Lett.**64**,821 (1990); T.L.Carroll and L.M.Pecora, IEEE Trans.Circuits Syst.**38**, 453 (1991).
[3] L. Kocarev, K.S. Halle, K. Eckert, L.O. Chua and U. Parlitz, Int. J. Bifurc. Chaos **2**, 709 (1992).
[4] R.He and P.G.Vaidya, Phys.Rev.A**46**, 7387 (1992).
[5] K.M.Cuomo and A.V.Oppenheim, Phys.Rev.Lett. **71**, 65 (1993).
[6] K.Murali and M.Lakshmanan, Phys.Rev.E **48**,R1624 (1993).
[7] K.Pyragas, Phys.Lett.A**181**, 203 (1993); A.Kittel, K.Pyragas, and R.Richter, Phys.Rev.E **50**, 262 (1994).
[8] K.Murali and M.Lakshmanan, Phys.Rev.E**49**, 4882 (1994).
[9] L.O.Chua, M.Itoh, Lj.Kocarev and K.Eckert, J.Circuits Syst. Computers **3**, 93 (1993).
[10] K.S. Halle, C.W. Wu, M. Itoh and L.O. Chua, Int.J.Bifurc.Chaos **3**, 469 (1993);U. Parlitz and L. Kocarev, Phys. Rev. Lett. **74**, 5028 (1995).
[11] S.Hayes, C.Grebogi and E.Ott, Phys.Rev.Lett.**70**, 3031 (1993).
[12] K.M.Cuomo, Int.J.Bifurc.Chaos **4**, 727 (1994).
[13] C.W. Wu and L.O. Chua, Int.J.Bifurc.Chaos **3**, 1619 (1993); Int.J.Bifurc.Chaos **4**, 979 (1994); IEEE Trans.Circ.Syst.-I**42**, 430 (1995).
[14] G.Perez and H.A.Cerdeira, Phys.Rev.Lett.**74**, 1970 (1995).
[15] N.F. Rulkov, M.M. Sushchik, L.S. Tsimring and H.D.I. Abarbanel, Phys.Rev.E**51**, 980 (1995).
[16] H.D.I.Abarbanel, N.F.Rulkov and M.M.Sushchik, Phys.Rev.E**53**, 4528 (1996).

[17] L.Kocarev and U.Parlitz, Phys.Rev.Lett. **76**, 1816 (1996).
[18] K.Murali and M.Lakshmanan, Int.J.Bifurc.Chaos **7**, (2) (1997); Phys.Rev.E (1997)(to appear).
[19] T.L.Carroll, J.F.Heagy and L.M.Pecora, Phys.Rev.E**54**, 4676 (1996).
[20] K.Pyragas, Phys.Rev.E. **54**, R4508 (1996).
[21] K.Murali, M.Lakshmanan and L.O.Chua, IEEE Trans.Circuits and Systems-I **41**, 462 (1994); Int.J.Bifurc.Chaos **4**, 1511 (1994);**5**, 563 (1995); M.Lakshmanan and K.Murali, Phil.Trans.Roy.Soc.London-Transactions **A353**, 33 (1995).
[22] M.N.Lorenzo, V.P.Munuzuri, V.P.Villar and K.Murali, Int.J.Bifurc.Chaos (1997) to appear.

FIGURE CAPTIONS

FIG. 1. Schematic digram showing the synchronization scheme using encryption key function.

FIG. 2. Generalized synchronization of a Chua's circuit (drive) and a MLC circuit(auxiliary). (a) y_2 vs y_1 of Chua's circuit($\alpha = 10.0$, $\beta = 14.87$), (b) z_2 vs z_1 of MLC circuit ($F = 0.15$, $\omega = 0.75$, $\epsilon = \epsilon_r = 1.3$). (c) z_1 vs y_1, (d) compound chaotic signal $d(t)$ vs y_1. Here y1,y2,z1,z2 and d(t) correspond to y_1, y_2, z_1, z_2 and $d(t)$ respectively in the text.

FIG. 3. (a) Difference signal $(y_{1r} - y_1)$ vs t for $\epsilon_r = 1.3$, (b) Difference signal $(z_{1r} - z_1)$ vs t, (c) Transmitted compound chaotic signal $d(t) = y_1 + s(t) + z_1$. Here $s(t) = 0.02 sin 0.5t$, (d) Recovered information signal $r(t)$ (using Eq.(40)). Here y1,y1r,z1,z1r,d(t) and r(t) correspond to $y_1, y_{1r}, z_1, z_{1r}, d(t)$ and $r(t)$ respectively in the text.

FIG. 4. (a) Compound chaotic signal $d(t) = y_1 + s(t) + y_2 z_1$ vs y_1 ($\alpha = 10, \beta = 14.87$, $F = 0.15$, $\omega = 0.75$, $\epsilon = \epsilon_r = 1.3$). Here $s(t) = 0.03 sin 0.2t$. (b) Transmitted compound chaotic signal $d(t)$, (c) Recovered information signal $r(t)$ (using Eq.(40)).

FIG. 5. (a) Digital information signal, (b) Transmitted compound chaotic signal $d(t) = y_1 + s(t) + y_2 z_1$, (c) Recovered digital information signal.

FIG. 6. (a) z_3 vs z_2 of Lorenz equations(41-43) ($\sigma = 10$, r=28, b=2.666), (b) compound chaotic signal $d(t) = (y_1 + z_1)$ vs y_1.

FIG. 7. (a) Difference signal $(z_{1r} - z_1)$ vs t, (b) Transmitted compound chaotic signal $d(t) = y_1 + s(t) + z_1$. Here $s(t) = 0.03 sin 0.2t$. (c) Recovered information signal $r(t)$.