Chaotic signal masking with arbitrarily fine recovery

Charles Tresser and Patrick Worfolk[1]

IBM, P.O. Box 218, Yorktown Heights, NY 10598

April 4, 1996

We describe a computer based method for chaotic signal masking which allows arbitrarily fine recovery of the masked message, as well as the masking of messages with large magnitude.

PACS numbers: 05.45.+b, 89.70.+c

[1]Current address: The Geometry Center, Unisversity of Minnesota, 1300 S. Second St., Minneapolis, MN 55454

This letter describes a new method to mask a signal before transmission and then recover it after reception. Prior work by Cuomo, Oppenheim, and Strogatz [1, 2], Wu and Chua [3, 4] and the authors [5] use synchronization properties [6, 7, 8] of various chaotic dynamical systems for this purpose. Chaotic signal masking as discussed in these papers and summarized later has been seriously attacked from the cryptographic point of view in Refs. [9, 10, 11] and we do not pretend to cure all nor even part of the problems, although our methods seem versatile enough to improve on secrecy. As described in Refs. [12, 13], there are applications other than secrecy for which the possibility of masking a signal by chaotic data, and then recovering it, is valuable (*e.g.*, improved resistance to interference and greater channel sharing). Our signal masking method does not use synchronization, but uses aspects of coding of dynamical systems and related well known mathematics. Hayes *et al.* [14] take advantage of symbol sequences and chaotic dynamical systems to transmit information in a different way. For a specific chaotic dynamical system, they experimentally demonstrate that applying small perturbations can produce a trajectory with a prescribed symbol sequence. They encode a desired message in the signal by controlling the symbol sequence.

We first present the basic idea of our method in a simple setting. Consider the class of one-dimensional maps which arise naturally when studying the Guckenheimer and Williams geometrical model for the Lorenz equations (see, *e.g.*, [15]). One such map is pictured in Figure 1. To avoid technical complications, we will assume that the maps $f : [-1, 1] \to [-1, 1]$ have the following properties:

1. f has a single discontinuity at $x = 0$ and $\lim_{x\to 0^+} = -1$ and $\lim_{x\to 0^-} = 1$.

2. f is sufficently smooth on $[-1, 0)$ and $(0, 1]$.

3. $f'(x) > \beta > \sqrt{2}$ for all $x \neq 0$.

These maps have some strong chaotic and ergodic properties. For example, from condition 3, any interval is mapped onto $[-1, 1]$ after a finite number of iterations.

We now recall the symbolic dynamics associated to these maps. Let $I_0 = [-1, 0)$ and $I_1 = (0, 1]$. To each $x \in [-1, 1]$ we can associate a sequence $\{\sigma_i\}_{i=0}^{\infty}$ of 0's and 1's defined by $\sigma_i = j$ if $f^i(x) \in I_j$. For the ease of discussion, we will ignore the minor

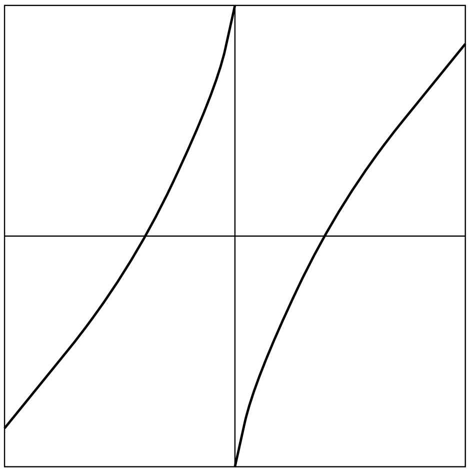

Figure 1: A simple expanding map.

complication which arises if the orbit of x includes 0. Excluding these points, every x has a unique symbol sequence, which are different for different x. If we order the symbol sequences in the natural way corresponding to binary expansions $(\sigma_0.\sigma_1\sigma_2\ldots)$, then the ordering of the points in $[-1,1]$ is preserved in the ordering of their symbol sequences.

Thus given a map f and the symbol sequence of a trajectory, the initial condition (and hence the whole trajectory) may be determined. Now suppose that $\{x_0, x_1, x_2, \ldots\}$ is a trajectory and let $\{s_0, s_1, s_2, \ldots\}$ be a signal which you would like to mask using the first trajectory. If you combine x_i and s_i to produce a y_i so that $\mathrm{sign}(y_i) = \mathrm{sign}(x_i)$ and that s_i is recoverable from knowledge of x_i and y_i then masking is easily accomplished. For example, if all the s_i are positive then one scheme is to add or substract s_i from x_i depending on the sign of x_i.

From knowledge of $\{y_i\}$, we can determine the symbol sequence associated with the point x_0. From uniqueness of symbol sequences, the point x_0 is identified and then the trajectory $\{x_i\}$ can be reconstructed. From the knowledge of $\{x_i\}$ and $\{y_i\}$, the signal $\{s_i\}$ is recovered. To exactly identify x_0 an infinite amount of data is necessary, but to identify it up to any arbitrarily small precision only a finite number of terms in its symbol sequence is necessary. An upper bound for this may be determined from

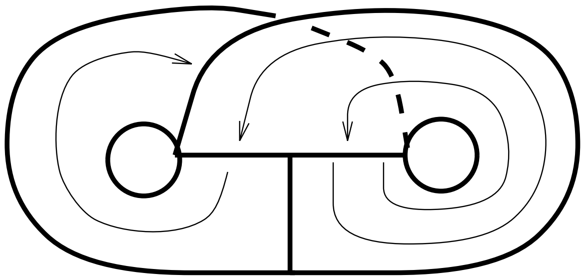

Figure 2: The Lorenz template.

the required precision and the lower bound, β, on the expansion of the map f.

Remark: The final s_i's of the message will be known with less and less precision except if identical arithmetic models are used to perform the computations at both ends and the x_i are computed using full precision.

Moving on from this simple setting, we consider semiflows on branched manifolds. For definiteness, we will consider semiflows on the Lorenz template, a branched two manifold pictured in Figure 2. Such semiflows occur as models for the flow in the Lorenz equations that arise from the geometric Lorenz attractor as described by Guckenheimer and Williams. The one-dimensional return map on the branch cut on the Lorenz template has properties 1-3 previously given. We can prescribe such semiflows by defining flows on each of the two planar portions of the branched manifold. This is pictured in Figure 2.

We place the branch cut at $[-1,1] \times 0$, and assume that the hole has width 4α. The exact details of the flow from $[0,1] \times 0$ to $[-1,1] \times 0$ are not important. In fact it is sufficient that simply a continuous curve be assigned for each initial point (not necessarily coming from a flow) so that the return map f has properties 1-3. We shall assume that the flow looks somewhat like that pictured in Figure 2.

Take one such flow satisfying the above criteria. This specifies a one-dimensional map f. Let $(x(t), y(t))$ be a trajectory of the system defined and assume that $(x(0), y(0)) \in [-1,1] \times 0$. We can define a symbol sequence to each trajectory which depends on whether the trajectory circles around the left or right hole. This symbol sequence is the same one as for the induced map f for the point $x(0)$. Thus from knowledge of only the symbol sequence of $(x(t), y(t))$ we may determine $x(0)$ and thus reconstruct the trajectory $(x(t), y(t))$. Notice, that $x(t)$ by itself determines the symbol sequence.

Now let $s(t)$ be a signal such that $|s(t)| < \alpha$. Consider the sum $T(t) = x(t) + s(t)$. Due to the limited magnitude of $s(t)$ and the width of the hole, the symbol sequence of $x(t)$ can be determined from $T(t)$. Then, $x(0)$ may be uniquely determined. Thus we see that from knowledge of the flow and $T(t)$, we can recover $x(t)$ and, consequently, $s(t)$. The explicit strategy for determining the symbol sequence from $T(t)$ is as follows.

I. Wait until $|T(t)| > 1 + 3\alpha$. When it is, if $T(t) > 0$ then mark a right symbol, else mark a left symbol. Continue to step II.

II. Wait until $|T(t)| < 1 + \alpha$. Return to step I.

The easiest way to see that this works is to consider the trajectory to be circling one the holes whenever $|x(t)|$ exceeds $1 + 2\alpha$. The trajectory cannot circle a hole without $|x(t)|$ exceeding $1 + 4\alpha$ which means that $|T(t)| > 1 + 3\alpha$. When $|(T(t)| > 1 + 3\alpha$, we have $x(t) > 1 + 2\alpha$ so the trajectory is circling one of the holes. When the trajectory returns to the center, $|x(t)|$ will decrease below 1 and thus $|T(t)|$ will decrease below $1 + \alpha$. When $|T(t)| < 1 + \alpha$, then $|x(t)| < 1 + 2\alpha$ so the trajectory is not circling a hole. Thus the strategy above will give the correct symbol sequence.

For the sake of comparison, we now describe how synchronization has been used for signal masking in previous works [1, 2, 3]. Suppose that the system

$$\dot{x} = f(x, \eta(t))$$

with $N_1, N_2 > 0$ and for all continuous $\eta(t)$ such that $||\eta||_\infty < N_1$, with the unique solution $x(t, x_0, t_0; \eta)$ satisfying $x(t_0, x_0, t_0; \eta) = x_0$ has the following properties:

1. For all $\epsilon > 0$ there exists a $\delta(\epsilon) > 0$ such that $||x(t, x_0, t_0) - x(t, x_1, t_0)|| < \epsilon$ whenever $||x_1 - x_0|| < \delta(\epsilon)$ and $||x_0||, ||x_1|| < N_2$.

2. There exists a $\delta > 0$ such that for all $\epsilon > 0$ there exists a $T(\epsilon) > 0$ such that $||x(t, x_0, t_0) - x(t, x_1, t_0)|| < \epsilon$ for all $t > t_0 + T(\epsilon)$ whenever $||x_1 - x_0|| < \delta$ and $||x_0||, ||x_1|| < N_2$.

Let $s(t)$ be a signal and $c(x, s(t))$ an invertible coding function, *i.e.,* there exists $d(c, x)$ such that $d(c(x, s(t)), x) = s(t)$, with the property that $||c(x, s(t))||_\infty < N_1$ whenever $||x(t)|| < N_2$. Now the following systems

$$\begin{aligned} \dot{x} &= f(x, c(x, s(t))) \\ \dot{y} &= f(y, c(x, s(t))) \end{aligned}$$

have the property that $||x(t) - y(t)|| \to 0$ as $t \to \infty$. Thus if one is given the signal $c(t) = c(x, s(t))$ and knows the dynamical system f, then the signal $y(t)$ can be constructed and we see that $||d(c(t), y(t)) - s(t)|| \to 0$ as $t \to \infty$. Consequently this defines a signal masking method which is easily unmasked by a receiver and relies on the synchronization of dynamical systems.

We shall now discuss the advantages and disadvantages of our signal masking method in comparison to the one derived from synchronization.

The synchronization method is analog and may be implemented in an electronic circuit, whereas our method may not. Thus coding and decoding are more strenuous for our method. For the synchronization method it is often hard to prove that the dynamical system has the desired asymptotic properties and produces an appropriate chaotic signal $x(t)$ so that the coded signal has the desired masking properties. The dynamics depends on the signal being sent and it is difficult to predict the effects. Notice, however, that techniques are given in Ref. [8] which allow for better synchronization properties of many dynamical systems. In our method, we have excellent control over the chaotic masking signal and may easily create a variety of different masks with very different signatures. The mask is independent of the message to be broadcast. For the synchronization method, the convergence of signals is asymptotic, so the first part of any broadcast message will be lost, whereas in our method the full signal can be reconstructed if the precaution is taken as described in the earlier Remark. We emphasize that in both these methods, knowledge of the initial condition of the chaotic system is not neeeded for decoding.

We thank Don Coppersmith for drawing our attention to Ref. [9].

References

[1] K. M. Cuomo and A. V. Oppenheim. Circuit implementation of synchronized chaos with applications to communications. *Phys. Rev. Lett.*, 71(1):65–68, 1993.

[2] K. M. Cuomo, A. V. Oppenheim, and S. H. Strogatz. Synchronization of Lorenz-based chaotic circuits, with applications to communications. *IEEE Trans. on Circuits and Systems*, 40(10):626–633, 1993.

[3] C. W. Wu and L. O. Chua. A simple way to synchronize chaotic systems with applications to secure communications systems. *Int. J. Bifurcations and Chaos*, 3(6):1619–1627, 1993.

[4] C. W. Wu and L. O. Chua. A unified framework for synchronization and control of dynamical systems. *Int. J. Bifurcation and Chaos*, 4(4):979–998, 1994.

[5] C. Tresser and P. A. Worfolk. Resynchronizing dynamical systems. Preprint, 1996.

[6] L. M. Pecora and T. L. Carroll. Synchronization in chaotic systems. *Phys. Rev. Lett.*, 64(8):821–824, 1990.

[7] L. M. Pecora and T. L. Carroll. Driving systems with chaotic signals. *Phys. Rev. A*, 44(4):2374–2383, 1991.

[8] C. Tresser, P. A. Worfolk, and H. Bass. Master-slave synchronization from the point of view of global dynamics. *CHAOS*, 5(4):693–699, 1995.

[9] Th. Beth, D. E. Lazic, and A. Mathias. Cryptanalysis of cryptosystems based on remote chaos replication. In Y. G. Desmedt, editor, *Advances in Cryptology - CRYPTO '94*, pages 318–331, New York, 1994. Springer-Verlag. Lecture Notes in Computer Science 839.

[10] K. M. Short. Steps toward unmasking secure communications. *Int. J. Bifurcations and Chaos*, 4(4):959–977, 1994.

[11] G. Pérez and H. A. Cerdeira. Extracting messages masked by chaos. *Phys. Rev. Letters*, 74(11):1970–1973, 1995.

[12] N. Gershenfeld and G. Grinstein. Entrainment and communication with dissipative pseudorandom dynamics. *Phys. Rev. Lett.*, 74:5024–7, 1995.

[13] M. K. Simon. *Spread Spectrum Communications Handbook*. McGraw-Hill, New York, 1994.

[14] S. Hayes, C. Grebogi, E. Ott, and A. Mark. Experimental control of chaos for communication. *Phys. Rev. Lett.*, 73(13):1781–4, 1994.

[15] J. Guckenheimer and P. J. Holmes. *Nonlinear Oscillations, Dynamical Systems, and Bifurcations of Vector Fields*. Springer-Verlag, New York, 1983.