カオスを用いた秘話通信における情報信号の増幅作用の解析

3P－5

畠澤 泰成 松本 隆
早稲田大学理工学部電気電子情報工学科

1.Abstract
なんらかの信号（これ以後、情報信号）を裸でそのまま送信すると、悪意ある第三者に情報を盗み見られる恐れがある。Chaotic Masking とは、Master 系（カオス性を有する信号を生み出す）と、Slave 系（カオス性を有する信号と、情報信号を分ける）の二つの同期したシステムを用い、作り出した信号を用いて情報信号を覆い隠す（Masking）ことによって、情報を安全に伝送する手法である。

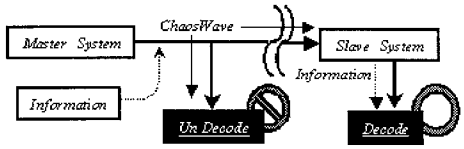

Fig.1 Concept of Chaotic Masking

2.R-L-Diode Circuit を用いた Chaotic Masking

Chaotic Masking のブロック図を Fig.2 に示す。使用する電流 i_m、これを情報信号に覆い被せ、送信する信号とする（以後、送信信号）。このとき、情報信号の振幅の大きさは電流 i_m の約 1/50 とする。

j（= 情報信号 + i_m）から Slave 系を流れる電流 i_S が生み出される。そして

復元信号 = j - i_S = 情報信号 + (i_m - i_S)

であり、(i_m - i_S)が小さければ小さいほど、復元信号は誤差が少なく、正しく復元できる。

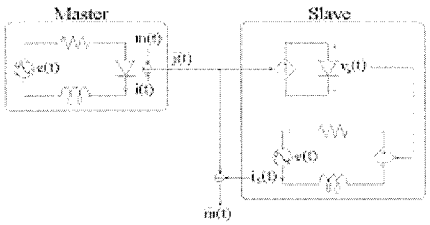

Fig.2 Circuit of Chaotic Masking

Amplification of information signals in Chaotic Masking
Yasunari Hatasawa, Takashi Matsumoto
Department of Electrical Electronics an Computer Engineering, WASEDA University
3-4-1 Okubo Shinjuku-ku Tokyo, 169-8555, Japan

$$\text{Master System}:\begin{cases}\dfrac{dq_m}{dt}=i_m-g(f(q_m))\\ L\dfrac{di_m}{dt}=-Ri_m-f(q_m)+E\sin(2\pi ft)\end{cases}$$

$$\text{Slave System}:\begin{cases}\dfrac{dq_s}{dt}=j-g(f(q_s))\\ L\dfrac{di}{dt}=-Ri-f(q_s)+E\sin(2\pi ft)\end{cases}$$

$$j=i_m+Information$$

Dynamics of Chaotic Masking

3.復元信号での誤差

2. で示した回路を用いた実験結果を Fig. 3 に示す。、伝送信号では情報信号が大変よく覆い隠されているが、復元信号では情報信号に対して、約 100 倍もの激しい増幅が起こっている。この増幅現象を調べるために、シミュレーションを用いて、三つの周波数を持つ情報信号の送信実験を行った。シミュレーション結果を Fig. 4～6 に示す。

高周波数の送信は良好な結果を得たが、低周波数では増幅を起こし、特定の周波数帯では、まったく復元ができなかった。

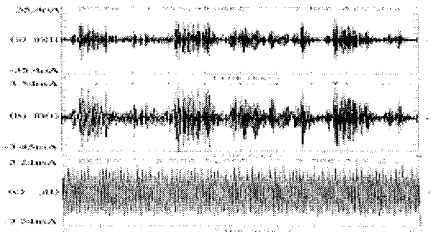

Fig.3 Experimental Result (a:Information signal
b :transmit signal c: decoded signal)

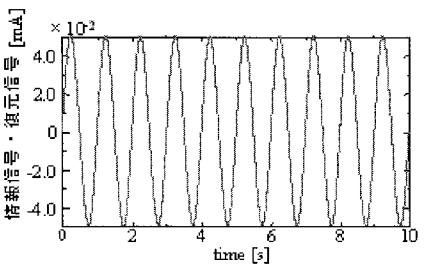

Fig.4 Simulation(Info = sin(2πft), f = 10[MHz])

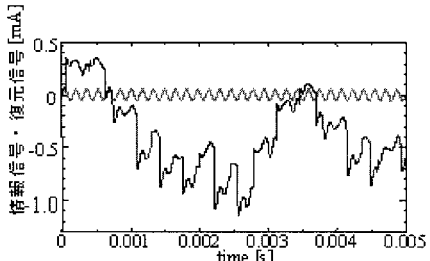

Fig.5 Simulation(Info = $\sin(2\pi ft)$, f = 10[kHz])

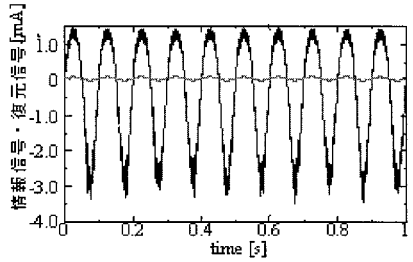

Fig.6 Simulation(Info = $\sin(2\pi ft)$, f = 10[Hz])

4.同期誤差の導出

情報信号の周波数に依存して、復元状態が変化することが解った。さらなる解析を行うため、Chaotic Masking を二つの系としてではなく、一つの系として捉える。そのために二つの値を新たに定義した。(Fig. 7)。

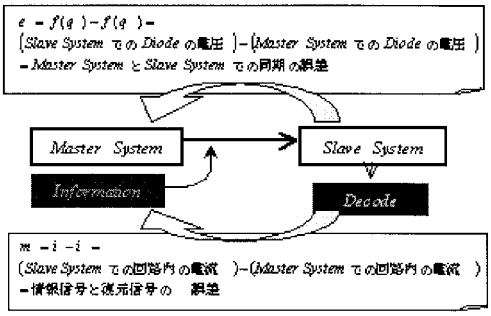

Fig.7 Synchronize error

この二つの誤差を用いて、先ほどの Chaotic Maskig の Dynamics を変形する。実際には、

(Slave 系の Dynamics)―(Master 系の Dynamics)

である。

そして、得られた Dynamics に線形近似等の近似を行うことによって、解析をより容易に行えるように変形を施した。

$$L\frac{dm_s}{dt} = -Rm_s(t) - e_s(t)$$

$$\frac{de_s}{dt} = -(g(f(q_s(t))) - g(f(q(t)))) + \underbrace{m(t)}_{\text{情報信号}}$$

ここで、g(f(q))の項に対して近似を行う

$$(g(f(q_s(t))) - g(f(q(t)))) \approx (g'(f(q_s(t))) - g'(f(q(t))))(f(q_s) - f(q_m)) = a(t)e_s$$

このa(t)におけるexp項は常に≒1ということがシミュレーションにより確かめられているので

$$a(t) = g'(f(q_s(t))) - g'(f(q_m(t))) = -\frac{I_s f(q_s(t))}{kT}\exp\left(\frac{q_s(t)f(q_s(t))}{kT}\right) - \frac{I_s f(q_m(t))}{kT}\exp\left(\frac{q_m(t)f(q_m(t))}{kT}\right) \approx -\frac{I_s f(q_s(t))}{kT} - \frac{I_s f(q(t))}{kT} = -\frac{I_s}{kT}(f(q_s(t)) - f(q_m(t)))$$

よって、

$$L\frac{dm_s}{dt} = -Rm_s(t) - e_s(t)$$

$$\frac{de_s}{dt} = -\frac{I_s}{kT}e_s + m(t)$$

この二つの誤差を Fig. 9 に示す。

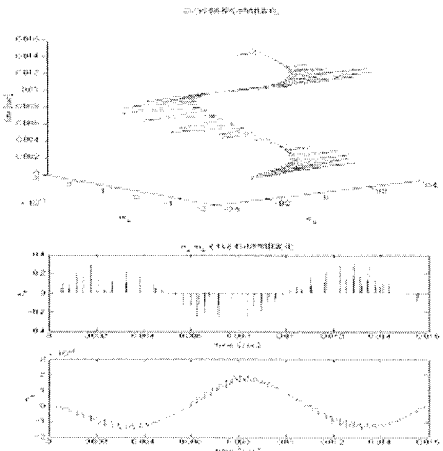

Fig.8 e_s, m_s

5. まとめ

今回は、Chaotic Masking の同期の誤差である二つの値を定義し、その振る舞いを調べた。この二つの誤差を調べることによって、復元信号における情報信号の周波数依存性が理論的に解析できると思われる。この結果は別途報告する。

参考文献

1.T. Matsumoto, and M. Nishi "Subsystem Decreasing for Exponential Synchronization of Chaotic Systems", Physical Review E, vol. 59, No. 2-A, pp.1711 - 1718, Feb. 1999